

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE INGENIERÍA INDUSTRIAL

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA



**PROYECTO DE REDISEÑO DE LA RED DE COMPUTADORAS DEL
HOSPITAL III JOSE CAYETANO HEREDIA UTILIZANDO VLANS**

PRESENTADA POR:

FRANK GARCIA ESPINOZA

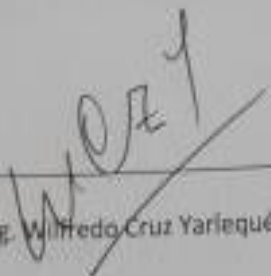
TESIS PARA OPTAR EL TÍTULO DE
INGENIERO INFORMÁTICO

Piura, Perú

2018

Tesis presentada como requisito para optar el título de Ingeniero Informático.

Asesor:



Ing. Wilfredo Cruz Yarlequé

Tesista:



Bach. Frank Garcia Espinoza



UNIVERSIDAD NACIONAL DE PIURA
FACULTAD DE INGENIERIA INDUSTRIAL
DECANATO



ACTA DE SUSTENTACIÓN DE TESIS

Los Miembros del Jurado Calificador de la Tesis denominada: «**PROYECTO DE REDISEÑO DE LA RED DE COMPUTADORAS DEL HOSPITAL III JOSÉ CAYETANO HEREDIA UTILIZANDO VLANS**», presentado por **FRANK GARCÍA ESPINOZA**, Bachiller en **INGENIERÍA INFORMÁTICA**, asesorado por el **ING. WILFREDO CRUZ YARLEQUÉ** y co asesorado por el **ING. JHONNY WILLIAMS CARRILLO LEJABO**, Reunidos para la sustentación de ésta y luego de escuchar su exposición y las respuestas a las preguntas formuladas, la declaran:

Con el Calificativo:

Aprobado
Sobresaliente

En consecuencia el sustentante se encuentra **apto** para recibir el título profesional de **INGENIERO INFORMÁTICO** conforme a Ley.

Piura, 17 de Abril del 2018

Dr. PEDRO ANTONIO CRIOLLO GONZALES
PRESIDENTE – JURADO CALIFICADOR

ING. JORGE ALVARADO TABACCHI
VOCAL – JURADO CALIFICADOR

ING. MARTÍN EDUARDO HERRERA LOZADA
SECRETARIO – JURADO CALIFICADOR

**"PROYECTO DE REDISEÑO DE LA RED DE COMPUTADORAS DEL
HOSPITAL III JOSE CAYETANO HEREDIA UTILIZANDO VLANS"**

TESIS PRESENTADA COMO REQUISITO PARA OPTAR EL TÍTULO DE:

INGENIERO INFORMÁTICO

APROBADO POR:

PRESIDENTE


Dr. PEDRO ANTONIO CRIOLLO GONZALES

VOCAL


ING. JORGE ALVARADO TABACCHI

SECRETARIO

ING. MARTÍN EDUARDO HERRERA LOZADA

DEDICATORIA

A mis padres el señor Jorge Luis García Espinoza y a la señora Mercedes Espinoza Dioses, a quien les dedico de forma muy especial este trabajo, por su constante e incondicional apoyo, por sus consejos y estímulo, por su paciencia y bondad, por lo que tengo que agradecerle infinitamente todo lo que soy.

Por todo ello, muchas gracias.

AGRADECIMIENTOS

Agradecer a Dios por cuidarme siempre y por darme la fortaleza para seguir adelante cada día.

Agradecer de manera muy especial a mi asesor, Ing. Wilfredo Cruz Yarlequé por haberme brindado el apoyo necesario en el planteamiento y realización de mi tesis, a quien le debo el éxito de este nuevo logro en mi vida profesional.

A mi amigo Ing. Jhonny William Carrillo Lejabo por apoyarme con la idea de realizar este proyecto y por el seguimiento constante del mismo.

A mi jurado de tesis: Dr. Pedro Criollo, Ing. Jorge Alvarado, Ing. Martín Herrera por su gran aporte y contribución al desarrollo de este trabajo de investigación.

A los docentes que me formaron profesionalmente durante mi vida universitaria, muchos de los cuales ahora son grandes amigos y serán mis futuros colegas.

A mis padres y a mis hermanos porque siempre buscan lo mejor para mí y me apoyan incondicionalmente.

A todos ellos, le estoy eternamente agradecido.

RESUMEN

El proyecto de investigación tiene como objetivo principal realizar un rediseño de topología de la red de computadoras utilizando VLANs que permita optimizar los recursos computacionales con la que cuenta el hospital mediante un análisis de la infraestructura, los requerimientos, y el planteamiento de un diseño que satisfaga las necesidades que actualmente requiere el hospital mediante la utilización de la tecnología de las VLANs, además proponer recomendaciones de políticas de administración y seguridad de la red informática, escalabilidad y la adaptabilidad que son impulsores clave.

En el desarrollo de la simulación del rediseño de red de computadoras se hizo uso del simulador Cisco Packet Tracer, conocido por ser una herramienta que permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

Primero, se identificaron los procesos relacionados a la gestión de la red dentro del hospital revisando los mismos, posteriormente se determinaron los requerimientos del rediseño de red. Asimismo, se resolvió que implementar vlans al rediseño sería una óptima solución.

En la simulación se tomaron en cuenta los equipos que conforman la red, su cableado estructurado y se hicieron las pruebas de funcionamiento respectivas.

El rediseño sin duda permite a la Jefatura División de Soporte Informático evaluar la propuesta que genera una mejora en los procesos.

Por lo tanto, se presenta una propuesta basada en VLAN's, esta solución cubre las necesidades del Hospital tanto en el aspecto funcional como en el aspecto relacionado a los costos, ya que el valor de los switches provistos en esta tesis están acorde al mercado actual de las comunicaciones.

Palabras Claves: Simulacion, VLAN, switch.

ABSTRACT

This research project has as main objective to redesign the topology of the computer network using VLANs to improve performance, scalability and adaptability as they are key drivers for the growth of the Hospital III Jose Cayetano Heredia network.

In the development of the simulation of computer network redesign, the Cisco Packet Tracer simulator was used, known as a tool that allows users to create network topologies, configure devices, insert packages and simulate a network with multiple visual representations.

First, the processes related to the management of the network within the hospital were identified, and the network redesign requirements were subsequently determined. Also, it was resolved that implementing vlans to redesign would be an optimal solution.

The simulation took into account all the equipment that make up the network, its structured wiring and the respective functional tests were done. Finally, the established indicators were evaluated by performing the respective tests in the simulation to ensure the success of the hypothesis.

The redesign undoubtedly allows the Head of IT Support Division to evaluate the proposal that generates an improvement in the processes

Therefore, a proposal based on VLANs is presented, this solution covers the needs of the Hospital in both functional and cost aspects, since the value of the switches provided in this thesis are in line with the current market of the communications.

Palabras Claves: Simulation, VLAN, switch.

ÍNDICE DE CONTENIDO

INTRODUCCIÓN	15
CAPÍTULO 1: EL PROBLEMA DE LA INVESTIGACIÓN	16
1.1 Descripción del Problema.....	16
1.2 Formulación del Problema.....	17
1.3 Objetivos de la Investigación	17
1.3.1 Objetivo General.....	17
1.3.2 Objetivos Específicos.....	17
1.4 Delimitación.....	17
1.5 Análisis económico	18
1.6 Análisis costo - beneficio.....	18
1.7 Análisis de factibilidad	24
1.8 Justificación de la Investigación	25
1.9 Criterios para la segmentación de redes	26
1.10 Hipótesis de la investigación	27
1.11 Identificación y operacionlización de variables	27
CAPÍTULO 2: MARCO TEÓRICO	27
2.1 Antecedentes de la Investigación	27
2.2 El Hospital III José Cayetano Heredia	29
2.2.1 Reseña Histórica del Hospital III José Cayetano Heredia.....	29
2.2.2 Misión	30
2.2.3 Visión	30
2.2.4 Objetivos estratégicos del Hospital III José Cayetano Heredia	30
2.2.5 Organigrama	32

2.3	Bases Teóricas	33
2.3.1	Modelo OSI	33
2.3.2	Protocolo TCP/IP.....	35
2.3.3	Dispositivos de red	36
2.3.4	Internet Protocol - IP	39
2.3.5	MAC.....	39
2.3.6	Host	40
2.3.7	Protocolo de Configuración de Hosts Dinámico – DHCP.....	40
2.3.8	Ethernet	41
2.3.9	Dominio de Broadcast	42
2.3.10	Dominio de Colisión.....	42
2.3.11	Modelo Jerarquico CISCO	42
2.3.12	Red de Área Local Virtual.....	46
2.3.13	Metodología Cisco.....	61
2.3.14	Herramienta de Simulación.....	62
CAPÍTULO 3: METODOLOGÍA Y DISEÑO DE LA INVESTIGACIÓN		64
3.1	Clase y diseño de investigación	64
3.1.1	Clase de investigación.....	64
3.1.2	Diseño de investigación	64
3.2	Población de investigación	64
3.3	Ubicación y descripción de la población	65
3.4	Técnicas e instrumentos para obtener datos	65
3.5	Metodología para el procesamiento y análisis de datos.....	65
CAPÍTULO 4: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN		67
4.1	Análisis del estado actual de la red.....	67
4.2	Metas del diseño de red	67
4.3	Metas técnicas.....	67

4.4	Ámbito.....	67
4.5	Restricciones.....	68
4.6	Uso actual de la red.....	68
4.7	Direcciones IP disponibles.....	70
4.8	Rendimiento de la red.....	70
4.9	Latencia.....	71
4.10	Seguridad.....	71
4.11	Infraestructura de red	72
4.12	Diseño del modelo	76
4.12.1	Diseño lógico propuesto y topología de red	76
4.12.2	Creación de VLANs.....	78
4.12.3	Estructura del modelo según RFC	78
4.12.4	VLAN.....	80
4.12.5	Dispositivos.....	81
4.12.6	Configuración de equipos	82
4.13	Simulación y evaluación del modelo propuesto.....	82
4.13.1	Simulación y evaluación.....	82
	CONCLUSIONES	84
	SUGERENCIAS	85
	BIBLIOGRAFÍA	86
	ANEXOS.....	87
	ANEXO 1.....	87
	ANEXO 2.....	93
	ANEXO 3.....	94
	ANEXO 4.....	95

ANEXO 5.....	96
ANEXO 6.....	98
ANEXO 7.....	100
ANEXO 8.....	101
ANEXO 9.....	103
ANEXO 10.....	105
ANEXO 11.....	113
ANEXO 12.....	114
ANEXO 13.....	120
ANEXO 14.....	121

ÍNDICE DE FIGURAS

Figura 1: Organigrama del Hospital III Jose Cayetano Heredia	32
Figura 2: Comunicación Peer-to-Peer	34
Figura 3: Iconos de los Dispositivos de Red	36
Figura 4: Transmisiones Simultáneas en un Switch.....	38
Figura 5: Interconexión de Dispositivos de Red	39
Figura 6: Interconexión de Dispositivos de Red	41
Figura 7: Capas del Modelo Jerárquico Cisco.....	43
Figura 8: Estructura de Red definido por Jerarquía	45
Figura 9: Diferencia entre límite físico y VLAN.....	46
Figura 10: VLAN de Datos	49
Figura 11: VLAN Predeterminada	50
Figura 12: VLAN Nativa.....	51
Figura 13: VLAN de Administración	52
Figura 14: VLAN de Voz	54
Figura 15: Como conectar un telefono IP de Cisco	55
Figura 16: Métodos de pertenencia de una VLAN.....	56
Figura 17: VLAN basado en puerto.....	57
Figura 18: VLAN basado en MAC	58
Figura 19: VLAN basado en protocolo.....	59
Figura 20: Red Actual del Hospital III José Cayetano Heredia.....	75
Figura 21: Topología de red propuesta basada en VLANs	77

ÍNDICE DE CUADROS

Tabla 1 - Beneficios.....	18
Tabla 2 - Gastos	19
Tabla 3 - Flujo de Caja.....	19
Tabla 4 – Valor actual neto.....	20
Tabla 5 – Valor actual neto.....	21
Tabla 6 – Valor actual neto.....	21
Tabla 7– Plan de implementación	23
Tabla 8 - Técnicas e Instrumentos	66
Tabla 9 - Usuarios por área	68
Tabla 10 - Anexos Telefónicos por área.....	69
Tabla 11 - Interfaces de red disponibles	70
Tabla 12: Direcciones IP – Red actual.....	70
Tabla 13: Ancho de banda contratado	71
Tabla 14: Activos de red - Amenazas de seguridad.....	71
Tabla 15: Switch por agrupación de usuarios.....	73
Tabla 16: Modelo de direccionamiento IP	78
Tabla 17: Número de usuarios por comunidad que tendrán VLAN	79
Tabla 18: Comunidad de usuarios – VLANs – Dirección IP	80
Tabla 19: Equipos de red	81

INTRODUCCIÓN

El Hospital III José Cayetano Heredia es una institución que brinda servicios de salud de mediana y alta complejidad esencialmente a la población piurana.

Actualmente, en el hospital se genera gran cantidad de información, haciendo necesario el uso de muchos servicios como el servidor de correo, backups, recursos lógicos y físicos, telefonía IP, entre los que más se usan.

El intercambio continuo de información a nivel de datos, VoIP, video se ha vuelto tan indispensable que ha obligado a muchas empresas a tener un sistema de cableado estructurado que brinde facilidades de mantenimiento, reubicación, administración y protección de la información.

Sin embargo, tener un sistema de cableado estructurado que cumpla las normas y especificaciones no es garantía del manejo eficiente, integridad y privacidad de la información, por lo que el objetivo de la presente tesis es complementar el tratamiento de métodos de administración y protección de la información basados en la segmentación de la red por medio de la tecnología VLAN.

VLAN es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas).

La siguiente tesis consta de cuatro capítulos:

En el capítulo 1 se plantea el Problema de Investigación, el capítulo 2 incluye el Marco Teórico, el capítulo 3 se presenta la Metodología y Diseño de la Investigación para evaluar si es viable y factible la propuesta de un diseño lógico y físico.

En el capítulo 4 establece el Análisis e Interpretación de Resultados de la Investigación.

Por último, se establece las principales conclusiones y recomendaciones a las que se ha llegado para finalizar de manera satisfactoria la presente tesis.

CAPÍTULO 1: EL PROBLEMA DE LA INVESTIGACIÓN

1.1 Descripción del Problema

Hoy en día, las redes de datos de las entidades públicas tienen una mayor carga de tráfico debido al uso de sistemas integrados como ERP, base de datos, voz y video, entre otros que lleva consigo una latencia. Algunas causas habituales en un Hospital Público que provocan congestión en la red son las descargas y transferencia de archivos, transmisión de imágenes a los consultorios, entre otros.

La red del Hospital III José Cayetano Heredia no está ajena a este problema, esto ocurre porque algunos equipos de red están sobrecargados con un exceso de tráfico que lleva consigo una congestión en la red de área local. Si bien hay fallas de conexión en algunos switches debido a cableado dañado o mal ponchado esto sin duda lleva en algunos casos pérdida de información, la cual hace notar que es una red que no brinda seguridad. Veamos las evidencias de la red actual. (**ANEXO 1**)

Esto lleva consigo que la información que se trasmite a través de la red de área local depende de la ubicación física de los departamentos. Sobre todo utilizar un conmutador por cada departamento ya es redundante.

Sin duda, estos inconvenientes afectan al personal, que son los que día a día tienen que realizar actividades en la red de datos.

También afecta el desempeño de los sistemas informáticos entre otros, como son:

- *Sistemas de Archivo y Comunicación de Imágenes (PACS), por sus siglas en inglés: Picture of Archive and Communication System.*
- *Sistema de Gestión Hospitalaria.*
- *Sistema de Aseguramiento.*
- *Sistema de Administración Documentaria.*

En consecuencia, las actividades que se realizan en la red de datos del Hospital suelen ser deficientes, impidiendo así gozar de los recursos de la red.

1.2 Formulación del Problema

¿Cómo se pueden solucionar los problemas que atraviesa la red actual de computadoras del Hospital III José Cayetano Heredia?

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Proponer un nivel de mejora en la red de computadoras a través de un nuevo diseño de la red del Hospital III José Cayetano Heredia.

1.3.2 Objetivos Específicos

- Formular una mejora en la velocidad del tráfico de datos a partir de la utilización de VLANs.
- Proyectar el incremento de seguridad de la información que se transfiere y comparte en la red.
- Formular las mejoras en la implementación del cableado estructurado acorde a estándares internacionales: EIA/TIA568, ANSI/TIA/EIA568B.

1.4 Delimitación

El alcance del proyecto enmarca la propuesta de creación de una nueva topología en los departamentos mencionados en ámbito – Capítulo 4, en el simulador Packet Tracer de Cisco Systems con el fin de proyectar una mejora en la seguridad y calidad del servicio en la red actual de datos del Hospital III José Cayetano Heredia.

1.5 Análisis económico

En el análisis económico del proyecto se consideró el diseño de la topología, los costos de los equipos que se proponen y su operación. (**ANEXO 2**).

1.6 Análisis costo - beneficio

Es aquella que identifica los méritos propios del proyecto.

Los flujos de costo y beneficios utilizados para este tipo de proyecto.

En la siguiente tabla, se presenta los beneficios que se obtendrían si se concreta la implementación del rediseño de red, para lo cual se describe los criterios utilizados para calcular los valores que representan:

- **Tiempo**, se ha considerado ahorro del tiempo derivado de la reducción en períodos en que el personal realiza sus operaciones como envío de información a otro usuario de la VLAN, entre otros.
- **Mayor flexibilidad en la administración y en los cambios de la red**, ya que la arquitectura puede cambiarse usando los parámetros de los switches Cisco.
- **Aumento de la seguridad**, puesto que la información se encapsula en un nivel adicional y puede ser analizada.
- **Disminución en la transmisión de tráfico en la red.**

Tabla 1 - Beneficios

DESCRIPCION	MONTO
Reducción de mantenimiento	6,000.00
Reducción de personal técnico en cableado estructurado	15,000.00
TOTAL	21,000.00

Elaboración: Propia

La siguiente tabla presenta los gastos anuales a incurrirse con la implementación del rediseño de red:

Tabla 2 - Gastos

DESCRIPCION	VALOR ANUAL
Mantenimiento anual	900.00
Servicio de internet anual (250 mensual)	3,000.00
TOTAL	3,900.00

Elaboración: Propia

La siguiente tabla presenta el flujo de caja:

Flujo de caja:

Tabla 3 - Flujo de Caja

	ANO 0	ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	TOTAL
Egresos (Gastos)	59,090.24	3,900.00	3,900.00	3,900.00	3,900.00	3,900.00	78,590.24
Ingresos (Beneficio)		21,000.00	21,000.00	21,000.00	21,000.00	21,000.00	105,000.00
FLUJO NETO	-59,090.24	17,100.00	17,100.00	17,100.00	17,100.00	17,100.00	

Elaboración: Propia

Indices financieros

Valor actual Neto (VAN)

En Excel la función para el cálculo del VAN se llama VNA. Esta función devuelve el valor actual neto a partir de un flujo de fondos y de una tasa de interés.

Sintaxis:

=VNA(tasa de descuento;matriz que contiene el flujo de fondos futuros) + inversión inicial

Tabla 4 – Valor actual neto

DESCRIPCION	FLUJOS NETOS	AÑO	FLUJOS DESCONTADOS VAN=Sumatoria(FN/(1+i)^n))
Inversión inicial	-59,090.24	0	-59,090.24
Flujo año uno	17,100.00	1	17,100.00
Flujo año dos	17,100.00	2	17,100.00
Flujo año tres	17,100.00	3	17,100.00
Flujo año cuatro	17,100.00	4	17,100.00
Flujo año cinco	17,100.00	5	17,100.00
	TOTAL		26,409.76

Elaboración: Propia

VAN: 26,409.76

Donde:

- **FN:** Flujos netos
- **i:** Tasa de interés: 0%
- **n:** Periodo (años) = 5 años

RESULTADO: El VAN es positivo y mayor que cero, el proyecto se acepta.

Tasa Interna de Retorno (TIR)

Para poder hallar la TIR, utilizaremos Excel.

La función TIR devuelve la tasa interna de retorno de una serie de flujos de caja.

Debido a que Excel calcula la TIR mediante un proceso de iteraciones sucesivas, opcionalmente se puede indicar un valor aproximado al cual estimemos que se aproximará la TIR, si no se especifica ningún valor, Excel utilizará 10%.

Sintaxis:

=TIR(matriz que contiene los flujos de caja)

Tabla 5 – Valor actual neto

DESCRIPCION	FLUJOS NETOS	AÑO	FLUJOS DESCONTADOS VAN=Sumatoria(FN/(1+i)^n)
Inversión inicial	-59,090.24	0	-59,090.24
Flujo año uno	17,100.00	1	15,035.76
Flujo año dos	17,100.00	2	13,220.70
Flujo año tres	17,100.00	3	11,624.75
Flujo año cuatro	17,100.00	4	10,221.46
Flujo año cinco	17,100.00	5	8,987.57
TOTAL	85,500.00		

Elaboración: Propia

TIR: 14%

RESULTADO: El TIR es mayor que la tasa de interés por lo que el proyecto se acepta.

Periodo de recuperación de la inversión

Tabla 6 – Valor actual neto

DESCRIPCION	FLUJOS NETOS	AÑO	SUMATORIA DE FLUJOS NETOS
Flujo año uno	17,100.00	1	17,100.00
Flujo año dos	17,100.00	2	34,200.00
Flujo año tres	17,100.00	3	51,300.00
Flujo año cuatro	17,100.00	4	68,400.00
Flujo año cinco	17,100.00	5	85,500.00

Elaboración: Propia

RESULTADO: El periodo de recuperación es de 3 años 5 meses 15 días.

Relación Costo – beneficio

$$C / B = \frac{\frac{TOTAL}{INGRESOS}}{\frac{TOTAL}{EGRESOS}}$$

$$C / B = \frac{105,000.00}{78,590.24} = 1.34$$

RESULTADO: La relación C/B de acuerdo a la inversión se ganará 1.34, por lo que el proyecto es aceptable.

Resultados del análisis

De acuerdo a los cálculos obtenidos se tiene que el rediseño de la red de computadoras del Hospital III José Cayetano Heredia requeriría una inversión inicial de S/59,090.24 con un tiempo de vida del proyecto de 5 años, de lo cual se ha obtenido que el VAN es positivo, la TIR es de 14%, una relación costo beneficio de 1.34 y un periodo de recuperación de 3 años 5 meses 15 días.

El análisis revela que los beneficios obtenidos serían significativamente mayores que los costos incurridos por lo que financieramente la implementación es factible y se recomienda su ejecución.

Plan de implementación

Comprende los pasos a seguir durante la implementación de la propuesta, en el cual se ha definido las actividades a realizar los tiempos estimados de instalación, personas responsables, y cronograma de actividades. La tabla 7 define ciertas características.

Tabla 7– Plan de implementación

ACTIVIDAD	DESCRIPCION	TIEMPO	RESPONSABLE
Adquisicion de equipamiento	Adquisicion de equipos de comunicaciones, accesorios y materiales adicionales	20 días	División de Soporte Informático
Tendido de cableado	Comprende el tendido del cableado UTP, conectorizaciones y pruebas del cableado	8 días	División de Soporte Informático
Instalación de equipos	Especifica la instalación de equipos de comunicaciones en el hospital	4 días	División de Soporte Informático
Configuraciones generales de red	Comprende la implementación y configuración	8 días	División de Soporte Informático
Monitoreo y pruebas	Comprende el monitoreo, pruebas y ajustes finales	6 días	División de Soporte Informático
Capacitacion	Capacitación al personal técnico sobre las configuraciones	3 días	División de Soporte Informático

Elaboración: Propia

Se puede visualizar el cronograma de ejecución de las actividades. (**ANEXO 3**)

Normativa de acceso a la información y recursos.

Para llevar un mejor control y administración de la información, servicios y recursos tecnológicos se propone implementar la siguiente normativa de control a la información, servicios y recursos tecnológicos del Hospital III José Cayetano Heredia, la misma que debe ser cumplida por cada usuario.

- Cada usuario es responsable de la administración y cuidado de los recursos tecnológicos que la empresa le proporcione para realizar su trabajo.
- Es responsabilidad de cada usuario la custodia de la información que se genera en su actividad diaria.
- El uso a los recursos tecnológicos y el acceso a los servicios (Internet, etc.) deben ser utilizados con fines laborales y el acceso a los mismos debe ser controlado por cada usuario.

- Es obligatorio de cada usuario mantener los equipos tecnológicos como el departamento División Soporte Informático los entregue, para lo cual no se recomienda configurar equipos, cambiar contraseñas, entre otros.
- Todo cambio o requerimiento tecnológico debe ser solicitado al departamento División Soporte Informático.
- Los permisos, usuarios y contraseñas de acceso a los sistemas informáticos del Hospital III José Cayetano Heredia son confidenciales y asignados a cada usuario por lo que es responsabilidad de cada usuario su correcta administración.
- Cualquier inconveniente presentado en los recursos tecnológicos, servicios de comunicaciones o accesos a los sistemas se debe reportar al departamento División Soporte Informático quienes serán los únicos encargados de dar solución a los problemas presentados.
- Los respaldos de información de los usuarios se deben realizar una vez por mes en coordinación con el personal de Soporte Informático.
- Cualquier desconocimiento sobre el manejo de aplicativos, servicios o recursos tecnológicos, los usuarios deben solicitar ayuda al personal del departamento División Soporte Informático para su respectiva capacitación y solución de problemas.

1.7 Análisis de factibilidad

a) Factibilidad operativa

Enumeraré las diferentes consideraciones operativas, así tenemos:

- Existe colaboración por parte del personal funcionario y operativo del Hospital III José Cayetano Heredia.

- Los procesos que realizan diariamente los usuarios serán más eficientes debido a un mejor desempeño de la red de datos.
- El diseño propuesto cambiará de alguna manera los métodos actuales de trabajo, la rapidez de las operaciones en la red, la interconexión e intercambio de información con otras áreas.

b) Factibilidad técnica

Se cuenta con el personal adecuado para la realización del cableado estructurado, dentro de la propuesta económica se contempla la contratación temporal del personal que realice la configuración de los equipos Cisco, así como la persona que supervise que las instalaciones de la nueva red cumplan con los estándares propuestos.

Asimismo, la adquisición de los equipos y materiales se contempla en la propuesta económica para su posterior aprobación.

c) Factibilidad financiera

Se asume en el mejor de los casos que el Estado Peruano a través de EsSalud cuenta con la disponibilidad económica para sustentar el desarrollo de este proyecto de investigación.

Considerando que la red Asistencial en los últimos años ha venido creciendo. Por ello, al estar en crecimiento, es importante se vea apoyada en el uso de nuevas tecnologías para así fortalecer los objetivos institucionales.

1.8 Justificación de la Investigación

Conscientes de lo importante que es para las instituciones hoy en día contar con una red que sea segura y con rapidez en el tráfico de datos es que se busca presentar una propuesta de una nueva topología implementando la tecnología VLAN.

El presente proyecto está basado en el modelo jerárquico CISCO, así como también en conceptos y teorías que nos sirven de ayuda para evaluar el desempeño y el estado de la red, respaldándonos de un simulador, con la finalidad de obtener un sustento valido del proyecto que se va a llevar a cabo.

Cabe resaltar que el objetivo del presente proyecto radica en determinar cuál es el nivel de mejora de la red de datos del hospital a partir de la implementación de VLAN dentro de la propuesta de una nueva topología de red.

Asimismo, pongo en manifiesto la conformidad por parte del personal del Departamento de Soporte Informático del Hospital III José Cayetano Heredia. **(ANEXO 4).**

1.9 Criterios para la segmentación de redes

El criterio tomado para segmentar la red es que tendremos la facultad de administrar cada una de estos con diferente política de seguridad.

Los usuarios que se encuentran en el rango 192.168.10.0 – 192.168.70.0 son considerados en el segmento A ya que cuenta con un mayor ancho de banda debido a que hay un mayor flujo de información y que tiene la mayor cantidad de usuarios en la red y tienen que acceder a las siguientes prestaciones: **Sistemas de Archivo Y Comunicación de Imágenes (PACS) y Sistema de Gestión Hospitalaria.**

El segmento B que esta conformado por los usuarios que pertenecen al rango 192.168.80.0 – 192.168.130. Estan distribuidos en el segundo nivel del hospital por áreas y cuentan con menor flujo de información ya que acceden a las prestaciones: **Sistema de Aseguramiento y Sistema de Administración Documentaria.**

En ambos segmentos se establecieron políticas de seguridad.

1.10 Hipótesis de la investigación

El nuevo diseño de la red del Hospital III José Cayetano Heredia mejorará el rendimiento, gestión, escalabilidad y seguridad en la red de computadoras.

1.11 Identificación y operacionlización de variables

a) Variable Independiente

Diseño de la topología de la Red del Hospital III José Cayetano Heredia.

b) Variable Dependiente

Desempeño de la red actual del Hospital III José Cayetano Heredia.

CAPÍTULO 2: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

Veamos a continuación algunas investigaciones o referencias anteriores que guardan relación con el proyecto de tesis.

Arévalo C y Rojas G (2015), realizaron la tesis denominada “**VLAN en la Infraestructura de red de datos de la empresa Redondos S.A. – Huacho**”. Con este estudio buscaron incrementar la seguridad de datos y la información dentro de la red de datos de la empresa Redondos S.A., proponiendo un mejor control en el Dominio Broadcast y la Gestión de la Red, sugiriendo la implementación de una Red Virtual Local para lograr este objetivo. Se demostró que la implementación de VLAN proporciona una serie de beneficios como: Segmentación de red, división y control del dominio broadcast, división lógica de una LAN basada en la estructura y nivel organizacional, seguridad a nivel de la capa de Red es decir a nivel IP.

Molina R. (2012), con su investigación “**Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la Empresa Editora El Comercio Planta Norte**”, realiza un rediseño de redes VLAN con la finalidad de segmentar las áreas en subredes para un mayor nivel de protección, brindar seguridad (Listas de Control de Acceso ACL's), mejorar el consumo de ancho de banda (Calidad de Servicio QoS), implementar nuevos protocolos en tecnologías CISCO, instalar redes inalámbricas y nuevos servicios de transferencia de archivos (Protocolo de Transferencia de Archivos FTP).

Todo ello con el propósito de disminuir costos y elevar la productividad de la Planta Norte de la empresa Editora El Comercio, haciéndola más robusta y escalable ante un crecimiento tecnológico a mediano y largo plazo.

De la Torre B. (2011), realizó un proyecto de grado titulado “**Rediseño de la Red LAN del Hospital Belén de Trujillo**”. El objetivo general del proyecto era rediseñar la red LAN del hospital, partiendo de un análisis de la problemática actual, cuyos hechos más evidentes denotan una lentitud o latencia de la red, además de un cableado estructurado no estandarizado sin considerar los patrones de diseño mínimo. Para el desarrollo del proyecto se emplearon metodologías de tipo aplicada ya que en este estudio concluyó que para la implementación de una solución con VLAN es necesario que se asegure primero que a nivel físico (cableado + equipos activos + pasivos) se tenga un diseño de acuerdo a los parámetros. Se debe llegar a tener una situación final equivalente con una estandarización del cableado estructurado y los indicadores de evaluación del rendimiento de la red de acorde a lo generalmente aceptado y una evidente satisfacción de los usuarios.

El Rediseño permitió a los departamentos y secciones del hospital gestionar su flujo de datos eficazmente y sin lentitud alguna, agilizando y reduciendo el tiempo de fluido de datos, de la misma manera se logró llevar una mejor administración de los equipos hospitalarios y una mejor programación de las actividades de mantenimiento.

Díaz A. (2010), con su proyecto “**Diseño e Implementación de una red privada virtual para la Empresa Eléctrica Quito S.A**”, concluyó que la implementación de VLAN es una solución para cubrir las necesidades más urgentes en el aspecto de comunicación-seguridad en la red de datos de la Empresa Quito S.A. (E.E.Q.S.A); esta solución se encuentra en el dominio del modelo de referencia TCP/IP.

2.2 El Hospital III José Cayetano Heredia

2.2.1 Reseña Histórica del Hospital III José Cayetano Heredia

El Hospital III José Cayetano Heredia fue fundado durante el Gobierno Militar del General Juan Velasco Alvarado. Fue inaugurado por el Ministro de Salud Francisco Miro Quesada y la esposa del Presidente Sra. Consuelo Gonzáles de Velasco, el día 02 de octubre de 1974. El Hospital III José Cayetano Heredia tiene por finalidad dar cobertura a los asegurados y sus derechos habitantes, a través del otorgamiento de prestaciones de prevención, promoción, recuperación, rehabilitación, prestaciones económicas, y prestaciones sociales que corresponden al régimen contributivo de la Seguridad Social en Salud, así como otros seguros de riesgos humanos. Dentro del Hospital III José Cayetano Heredia se encuentra la Oficina de Soporte Informático cuyas funciones son formular las iniciativas y propuestas correspondientes a la Oficina para los Planes de Gestión y Presupuesto de la Red; identificar y sustentar las

necesidades informáticas requeridas para el cumplimiento de sus funciones, a fin de que sean proveídas por las respectivas jefaturas; facilitar la provisión y atención oportuna del soporte técnico para las áreas dentro de su entorno, informando oportunamente las acciones que permitan brindar una adecuada gestión informática a las áreas usuarias; garantizar el funcionamiento de los sistemas de información que están en las áreas usuarias dentro de su entorno; establecer procedimientos de seguridad y control interno informáticos para las áreas dentro de su entorno, a fin de proteger los sistemas de información, base de datos y demás recursos informáticos involucrados; actualizar el inventario físico de contratos, licencias, hardware, sistemas operativos, software de oficina y otros instalados en los equipos de cómputo y de telecomunicaciones de la red.

2.2.2 Misión

Somos una institución de seguridad social de salud que persigue el bienestar de los asegurados y su acceso oportuno a prestaciones de salud, económicas y sociales, integrales y de calidad, mediante una gestión transparente y eficiente.

2.2.3 Visión

Ser una institución que lidere el proceso de universalización de la seguridad social, en el marco de la política de inclusión social del Estado.

2.2.4 Objetivos estratégicos del Hospital III José Cayetano Heredia

Tomando como punto de partida la Visión, la Misión y los valores institucionales, se procedió a formular cuatro objetivos estratégicos que son aplicables a toda la institución y sus sistemas institucionales; su realización se plantea en el mediano plazo. Por estas características, son los objetivos

centrales de la institución en este periodo estratégico. A continuación, se detallan los cuatro objetivos estratégicos:

- **Objetivo estratégico 1:** Extender la cobertura de la seguridad social, incluyendo a los trabajadores independientes e informales.
- **Objetivo estratégico 2:** Brindar atención integral a los asegurados, con los más altos estándares de calidad, en el marco de un fuerte compromiso del Estado con el bienestar de los asegurados; mejorar el trato a los asegurados, cambiar el modelo de atención por uno basado en la atención primaria y actuar sobre los determinantes sociales de la salud, con énfasis en los aspectos preventivo–promocionales.
- **Objetivo estratégico 3:** Garantizar la sostenibilidad financiera de la seguridad social en salud.
- **Objetivo estratégico 4:** Implementar una gestión transparente basada en el mérito y la capacidad, con personal calificado y comprometido.

2.2.5 Organigrama

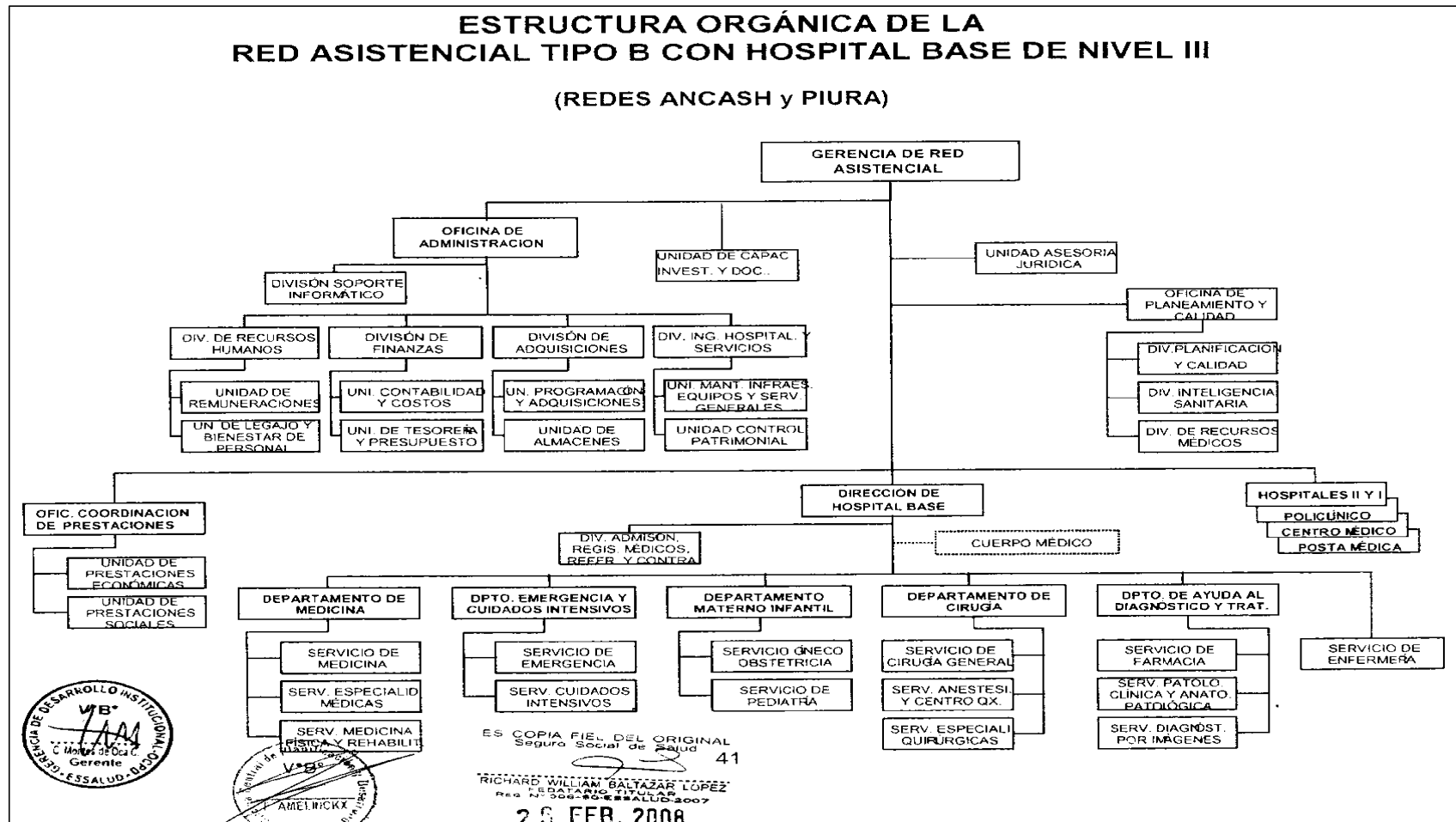


Figura 1: Organigrama del Hospital III Jose Cayetano Heredia

Fuente: División de Soporte Informático

2.3 Bases Teóricas

2.3.1 Modelo OSI

El Modelo OSI - Open Systems Interconnection es el modelo de red descriptivo de contiene siete capas definidas por la ISO, que asegura compatibilidad e interoperabilidad entre varias tecnologías de red producidas por indistintas compañías, lo que permite trabajar de manera independiente sobre funciones de red separadas y por ende disminuir su complejidad y acelerar su evolución. Las siete capas del modelo realizan diferentes funciones, las cuales son las siguientes:

1. **Capa Física:** Especifica voltajes, conectores, tasas de transmisión, medios de transmisión, entre otros.
2. **Capa de Enlace de Datos:** Utiliza las direcciones MAC para acceder a las estaciones finales, notifica errores, pero no los corrige
3. **Capa de Red:** Determina el mejor camino, utilizando direccionamiento lógico (IP).
4. **Capa de Transporte:** Provee una confiable o no confiable entrega de datos, ordena los segmentos que llegan en desorden.
5. **Capa de Sesión:** Establece, maneja y termina sesiones entre aplicaciones, asigna puertos lógicos.
6. **Capa de Presentación:** Traduce entre varios formatos de datos, encriptamiento, comprensión, entre otros.
7. **Capa de Aplicación:** Provee protocolos y software al servicio del usuario (Navegadores WEB, correo electrónico, etc).

Para que los datos viajen desde un origen a su destino, cada capa del modelo OSI en el origen debe comunicarse con su respectiva capa en el destino. Esta comunicación es conocida como peer-to peer. Durante este proceso, los protocolos de cada capa intercambian información denominada Protocol Data United (PDUs).

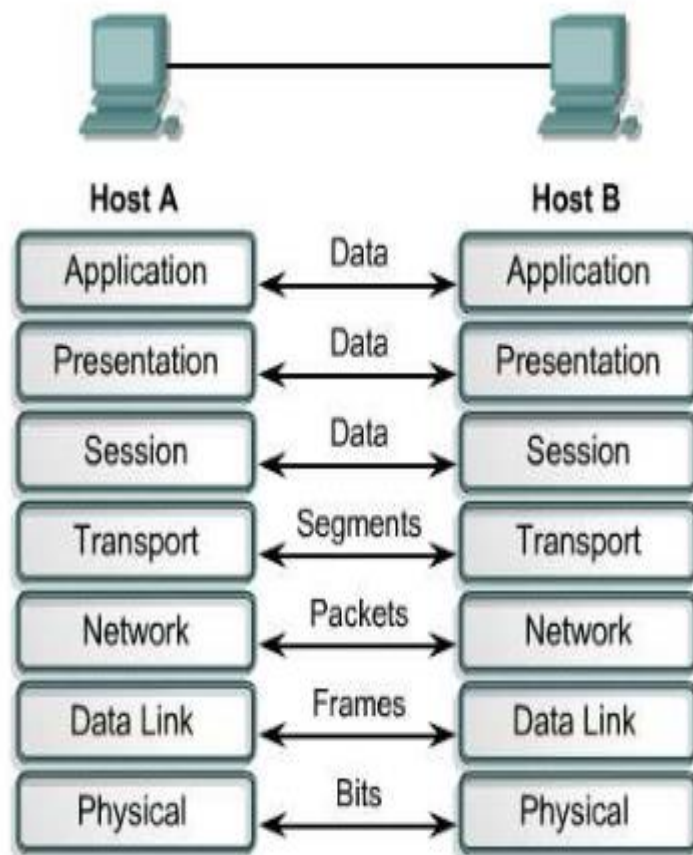


Figura 2: Comunicación Peer-to-Peer

Fuente: <http://www.cisco.netacad.net>

Existe un método llamado **encapsulación** que añade cabeceras y trailers a la data que va hacia debajo de la pila OSI. El dispositivo receptor le realiza un desnudo a la cabecera, que es la que contiene direcciones para esa capa a lo que llamaremos **desencapsulación**.

2.3.2 Protocolo TCP/IP

Según Abel Rodríguez Ávila (2007), el protocolo TCP/IP es el elemento que hace posible que los distintos ordenadores repartidos por el mundo y conectados a la red intercambien información. El protocolo que utiliza es el TCP/IP.

A cada ordenador se le asigna una dirección o nombre (dirección IP), única para cada uno de ellos e identificativa en la red.

En realidad, al hablar de TCP/IP, estamos hablando de dos protocolos diferentes que se combinan para facilitar el control y la transferencia en internet. El funcionamiento de este protocolo es muy sencillo.

En primer lugar, el protocolo TCP fracciona, en paquetes independientes, la información y los numera para que al llegar a su destino se ordenen correctamente. Otro dato importante que incluye es la denominada suma de comprobación, que coincide con el número total de datos que contiene el paquete. Esta suma sirve para averiguar en el punto de destino si se ha producido alguna pérdida de información. A continuación, el protocolo IP proporcionará a cada paquete, entre otras informaciones, las direcciones IP de origen y destino.

Según son enviados, cada paquete irá escogiendo el camino más adecuado para llegar a su destino. De este modo Internet se consolida como una red estable. Existen cientos de vías alternativas para un destino concreto, por lo que, aunque fallen ordenadores intermedios o no funcionen correctamente algunos canales de información, prácticamente los paquetes siempre llegarán a su destino.

2.3.3 Dispositivos de red

Stallings (2000) señala que existen dos clasificaciones, la primera clasificación, la primera clasificación son los dispositivos de usuario final, las cuales son las computadoras, impresoras, scanners y otros dispositivos que provean servicios directamente al usuario. Dichos dispositivos son conectados físicamente a la red usando una NIC (Network Interface Card).

Los dispositivos de red, considerados la segunda clasificación, proveen la comunicación entre dispositivos de usuario final. Veamos:

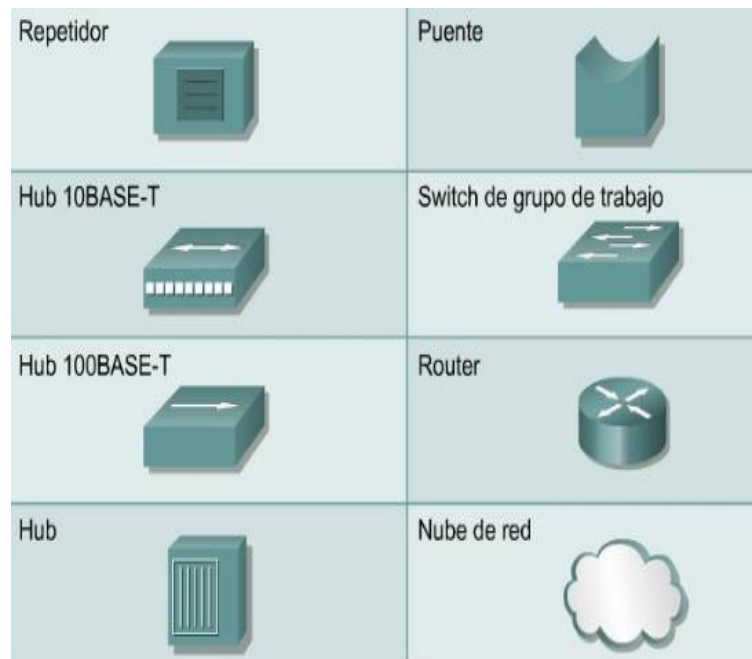


Figura 3: Iconos de los Dispositivos de Red

Fuente: <http://www.cisco.netacad.net>

- **Repetidor**

Dispositivo que regenera señales analógicas o digitales distorsionadas por la pérdida de transmisión. Pertenece a la capa 1.

- **Hub**

Dispositivo que permite la concentración de varios dispositivos dentro de un solo segmento. Amplifica las señales de datos para todos los equipos conectados excepto para el dispositivo que envió la señal. Pertenecce a la capa 1.

- **Bridge**

Dispositivo que separa dominios de colisión porque analiza las direcciones MAC para determinar si las tramas de datos pueden o no cruzar entre dos segmentos de red. Para lograr esto, el bridge aprende las direcciones MAC de los dispositivos en cada segmento conectado.

Pertenecce a la capa 2.

- **Switch**

Tanenbaum (2003) menciona que es un dispositivo de capa 2. Los switches toman las decisiones de envío basadas en las direcciones MAC contenidas dentro de las tramas de datos transmitidas. Los switches aprenden las direcciones MAC de los dispositivos conectados a cada puerto, a través de la lectura de las direcciones MAC origen que se encuentran en las tramas que ingresan al switch, luego esta información es ingresada dentro de la tabla de conmutación que es almacenada en la CAM. Los switches crean un circuito virtual entre dos dispositivos conectados que quieren comunicarse. Cuando este circuito virtual ha sido creado, un camino de comunicación dedicado es establecido entre los dos dispositivos, entonces se crea un ambiente libre de colisiones entre el origen y el destino lo cual implica la máxima utilización del ancho de banda disponible.

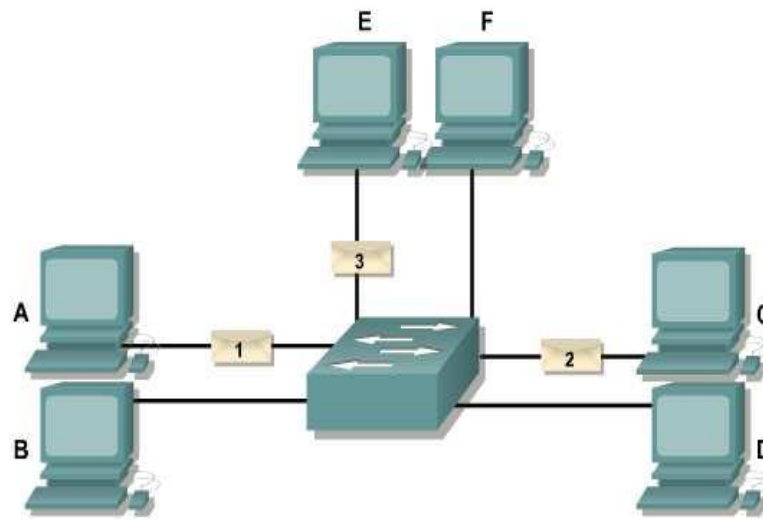


Figura 4: Transmisiones Simultáneas en un Switch

Fuente: <http://www.cisco.netacad.net>

- **Router**

Cisco Networkers Solutions Forum (2006). Se define dispositivo de capa 3 que toma decisiones basadas en direcciones de red. Estos utilizan tablas de ty para almacenar estas direcciones de capa 3. Los routers se encargan de elegir el mejor camino para enviar los datos a su destino y conmutar o enrutar los paquetes al puerto de salida adecuado.

Los routers dividen tanto dominios de broadcast como dominios de colisión. Además, son los dispositivos de mayor importancia para regular el tráfico, porque proveen políticas para la administración de la red con filtrado de paquetes de seguridad.

Además, dan acceso a redes de área ampliza (WAN), las cuales están destinadas a comunicar o enlazar redes de área local (LAN) que se encuentran separadas por grandes distancias.

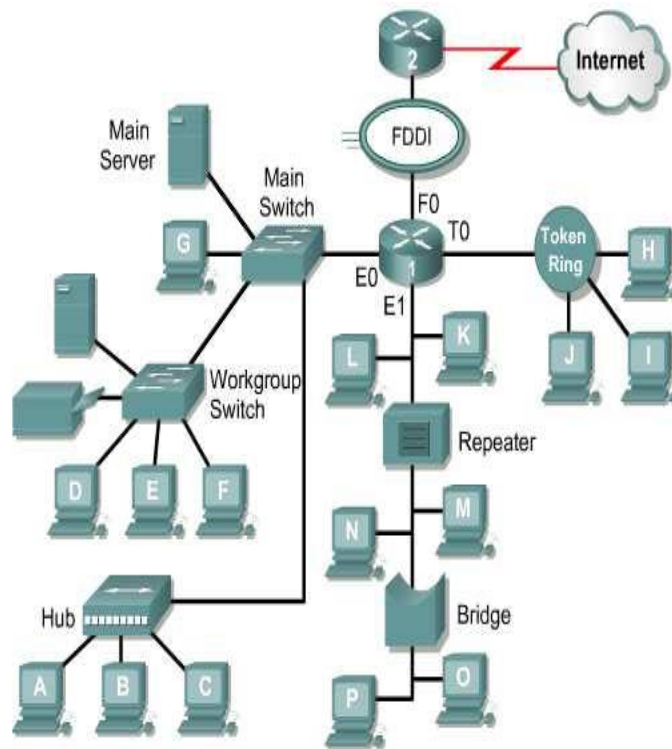


Figura 5: Interconexión de Dispositivos de Red

Fuente: <http://www.cisco.netacad.net>

2.3.4 Internet Protocol - IP

Es un número que identifica un dispositivo en una red (un ordenador, una impresora, un router, entre otros). Esos dispositivos al formar parte de una red serán identificados mediante un número IP único en esa red. El IP no cuenta con la posibilidad de confirmar si un paquete de datos llegó a su destino. Esto puede permitir que el paquete arribe duplicado, con daños, en un orden erróneo o que, simplemente, no llegue a destino.

2.3.5 MAC

Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

2.3.6 Host

La palabra inglesa host, que en español se traduciría como huésped, se usa en informática sobre todo a nivel de redes, donde en muchas ocasiones (no siempre), se asimila al concepto de servidor.

Un host no es más que un nodo, un ordenador o un conjunto de ellos, que ofrecen servicios, datos, al resto de ordenadores conectados a la red, sea esta local o global como internet. En el caso de redes locales, el host suele coincidir con el ordenador central que controla la red.

2.3.7 Protocolo de Configuración de Hosts Dinámico – DHCP

El DHCP está basado en el RFC 2131, y trabaja en modo cliente – servidor. El protocolo de configuración de hosts dinámico habilita a los clientes DHCP para obtener sus configuraciones desde un servidor DHCP, considerando que la opción de configuración de mayor importancia es la dirección IP asignada al cliente.

El DHCP no se utiliza para la configuración de los switches, routers o servidores. Estos hosts necesitan tener direcciones estáticas.

DHCP usa el UDP como protocolo de transporte. El cliente envía mensajes al servidor sobre el puerto 67, mientras que el servidor envía mensajes al cliente sobre el puerto 68. Los clientes DHCP arriendan la información del servidor por un periodo definido administrativamente. Y cuando el arrendamiento expira, el cliente debe pedir otra dirección, aunque generalmente se le reasigna la misma.

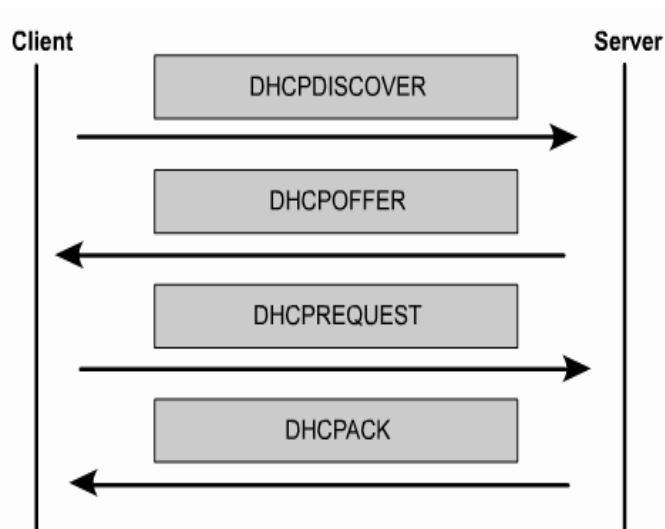


Figura 6: Interconexión de Dispositivos de Red

Fuente: <http://www.cisco.netacad.net>

2.3.8 Ethernet

Ethernet o su estándar equivalente IEEE 802.3 es básicamente una tecnología de transmisión broadcast, donde los dispositivos como computadoras, impresoras, servidores de archivos, etc; se comunican sobre un medio de transmisión compartido, lo que quiere decir que ellos se encuentran en una continua competencia por el ancho de banda disponible. Por lo tanto, las colisiones son una natural ocurrencia en redes Ethernet y pueden ocasionar un gran problema.

La entrega de tramas de datos Ethernet es de naturaleza broadcast. Ethernet usa el método CSMA/CD (Acceso Múltiple Sensible a Portadora con Detección de Colisión) que le permite a una sola estación transmitir y puede soportar tasas de transmisión de alta velocidad como: Ethernet: 10 Mbps, Fast Ethernet: 100 Mbps, Gigabit Ethernet: 1000 Mbps y 10-Gigabit Ethernet: 10.000 Mbps.

El desempeño de un medio compartido Ethernet/802.3 puede ser negativamente afectado por factores como las aplicaciones multimedia con alta demanda de ancho de banda tales como video e internet, que junto con la

naturaleza broadcast de Ethernet pueden crear congestión en la red, y la latencia normal que adquieren las tramas de viajar a través de los medios de red, atravesar dispositivos de red y los propios retardos de las NIC's.

2.3.9 Dominio de Broadcast

Para Romero, Concejero, Bengumea, Rivera, Roper, Sanchez, Siavines (2010), un dominio de broadcast es cuando todas las computadoras que están en un segmento de red pueden ver y recibir la información de las demás. Por ejemplo, si tienes un hub o un switch que mantienen un mismo segmento de broadcast, pues todas las computadoras ven la misma información. Si tienes un router, entonces divides el dominio de broadcast, pues el router separa las redes.

2.3.10 Dominio de Colisión

Para Romero, Concejero, Bengumea, Rivera, Roper, Sanchez, Siavines (2010), un dominio de colisión es área que se ve afectada cuando ocurre una colisión o "error" en la red. Si tienes un hub todos los segmentos tienen el mismo dominio de colisión. Si se produce una colisión todos los segmentos se verán afectados.

Si tienes un switch o un puente, entonces estás separando los dominios de colisión, pues el switch puede separar la información de cada red, entonces si se produce una colisión solo afecta a los dispositivos del mismo segmento.

2.3.11 Modelo Jerarquico CISCO

Consta de tres capas:

- Capa Nucleo: **Backbone**
- Capa de Distribución: **Routing**

- Capa de Acceso: **Switching**

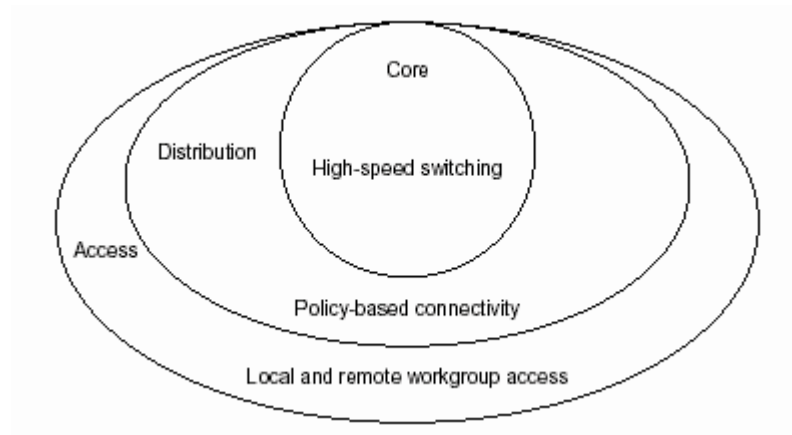


Figura 7: Capas del Modelo Jerárquico Cisco

Fuente: <http://www.cisco.netacad.net>

2.3.11.1 Capa Nucleo

Es el backbone de conmutación de alta velocidad que debe ser diseñado para conmutar paquetes lo más rápido posible, es decir, es responsable del transporte de grandes cantidades de tráfico en forma confiable y rápida, por lo tanto, la preocupación de esta capa es la velocidad y latencia. Es importante considerar, lo que no debemos hacer en esta capa:

- No realizar ningún tipo de manipulación de paquetes, tal como usar listas de control de acceso, enrutamiento entre redes de área local virtuales (VLAN) o filtro de paquetes, lo cuál reducirá el tráfico.
- No soporta accesos de grupo de trabajo.
- Evitar expandir el núcleo o *core* cuando la red crece. Si el desempeño es un problema en el *core*, son preferibles las actualizaciones en lugar de las expansiones.

2.3.11.2 Capa Distribución

También conocida como “workgroup layer”; y es el punto de comunicación entre la capa y el *core*. Las principales funciones de la capa de distribución son el proveer enrutamiento, filtros, accesos WAN y el determinar cómo los paquetes pueden acceder al *core* si es necesario.

La capa de distribución es donde se implementan las políticas para la red. Existen algunas acciones que generalmente deben hacerse en esta capa:

- Enrutamiento.
- Implementación de listas de control de acceso o filtro de paquetes.
- Implementación de seguridad y políticas de red, incluyendo traslado de direcciones y firewalls.
- Calidad de Servicio, en base a las políticas definidas.
- Redistribución entre protocolos de enrutamiento, incluyendo rutas estáticas.
- Enrutamiento entre VLANs y otras funciones que soportan los grupos de trabajo.
- Definición de dominios de broadcast y multicast.
- Posible punto para acceso remoto.
- Traslado de medios de comunicación.

2.3.11.3 Capa Acceso

La capa de acceso es el punto en el cual los usuarios finales son conectados a la red. Esta capa puede también usar listas de acceso o filtros para optimizar las necesidades de un grupo particular de

usuarios. Los recursos de red de la mayoría de usuarios deben estar disponibles localmente. Esta capa también es conocida como “*desktop layer*”. Estas son algunas de las funciones que incluye esta capa:

- Continúa el control de acceso y políticas (desde la capa de distribución).
- Creación de dominios de colisión separados (microsegmentación).
- Conectividad de los grupos de trabajo dentro de la capa de distribución.
- Habilitar filtros de direcciones MAC.
- También es posible tener acceso a grupos de trabajo remotos.
- Presta servicios de asignación de VLANs a nivel de capa 2 del modelo OSI.

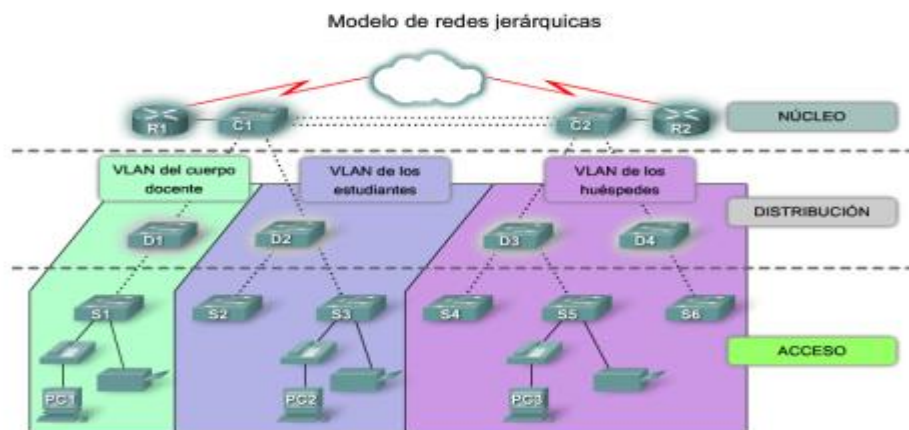


Figura 8: Estructura de Red definido por Jerarquía

Fuente: <http://www.cisco.netacad.net>

2.3.12 Red de Área Local Virtual

Para Tanenbaum (2003), es una agrupación lógica de dispositivos o servicios de red, en base a funciones, departamentos, equipos de trabajo o aplicaciones, sin considerar la localización física o conexiones de red.

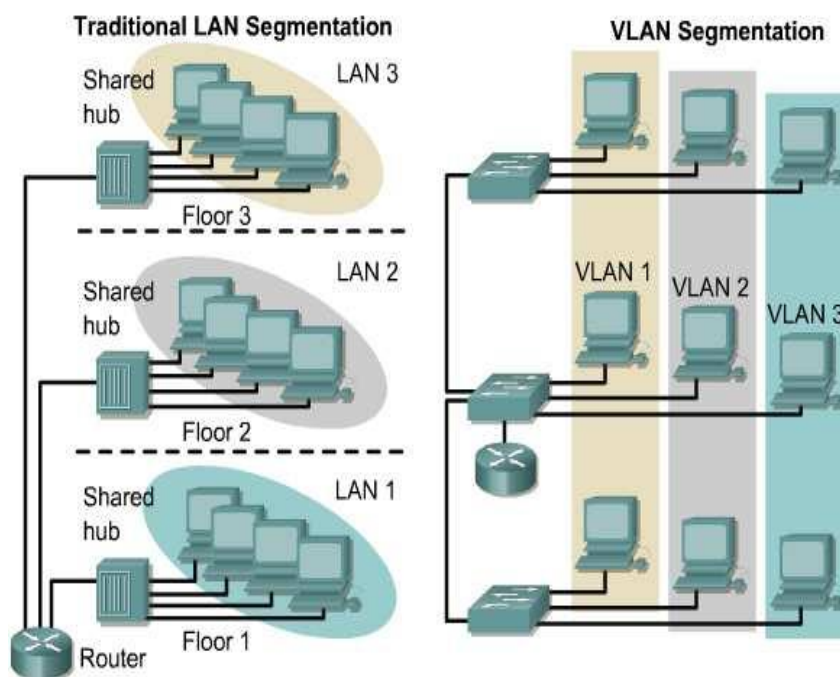


Figura 9: Diferencia entre límite físico y VLAN

Fuente: <http://www.cisco.netacad.net>

La principal actividad de las VLANs es una segmentación lógica de la red en diferentes dominios de broadcast, es decir que los paquetes son solamente conmutados entre puertos que han sido asignados a la misma VLAN.

Así como solo los routers proveen conectividad entre diferentes segmentos LAN, también solo los routers o equipos que operen en la capa tres del modelo OSI proveen conectividad entre diferentes segmentos VLAN. Los routers en topologías VLAN proveen filtrado de broadcast, seguridad y administración del flujo de tráfico.

2.3.12.1 Ventajas de las VLANs

- **Facilidad en la administración** de adición, movimiento y cambio de estaciones de trabajo en la red. (Flexibilidad, escalabilidad, facilidad de administración).
- **Incrementan el desempeño de la red** agrupando estaciones de trabajo, recursos y servidores según su función, sin importar si ellos se encuentran en el mismo segmento físico LAN.
- **Incrementan el número de dominios de broadcast** mientras éstos decrecen en su tamaño (mejor desempeño).
- **Mejoran la seguridad de la red**, porque solamente las estaciones de trabajo que pertenezcan a la misma VLAN podrán comunicarse directamente (sin enrutamiento).
- **Facilitan el control de flujo de tráfico**, porque permiten controlar la cantidad y tamaño de los dominios de broadcast, debido a que éstos por defecto son filtrados desde todos los puertos que no son miembros de la misma VLAN en un switch.
- **Mayor eficiencia del personal de TI:** las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando proporciona un switch nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular se implementan cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre.
- La configuración o reconfiguración de VLANs se realiza a través de software, por lo tanto, esto no requiere de movimientos o

conexiones físicas de los equipos de red (facilidad de administración).

2.3.12.2 Características de las VLANs

a. VLAN de rango normal

- Para redes de pequeñas y medianas empresa.
- ID de VLAN entre 1 y 1005.
- ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI, estas VLAN se crean automáticamente y no se pueden eliminar. Las configuraciones se almacenan en la **vlan.dat**, el cual se encuentra en la memoria flash del switch.

b. VLAN de rango extendido

- Son diseñadas para proveedores de servicios.
- ID de VLAN entre 1006 y 4094. Admiten menos características de VLAN que las VLAN de rango normal.
- Se guardan en el archivo de configuración en ejecución.

2.3.12.3 Tipos de VLAN

Actualmente, existe fundamentalmente una manera de implementar las VLAN: “**VLAN basada por puerto**”.

Una VLAN basada en puerto se asocia con un puerto denominado “acceso VLAN”.

Sin embargo, en redes existe una cantidad de términos para las VLAN. Algunos términos definen el tipo de tráfico de red que envían y otros definen una función específica que desempeña una VLAN.

A continuación, se describe la terminología común de las VLANs.

Tipos de VLAN

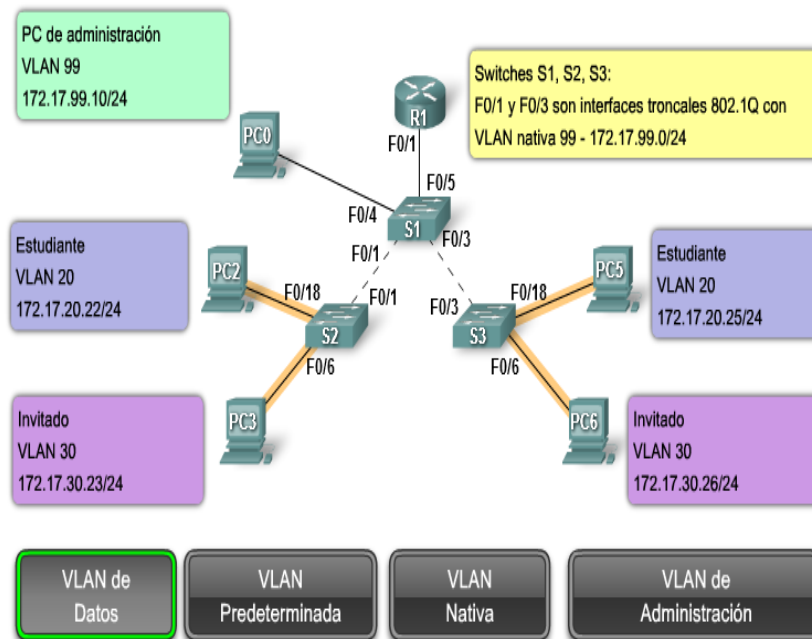


Figura 10: VLAN de Datos

Fuente: <http://www.cisco.netacad.net>

a. VLAN de Datos

Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces, a una VLAN de datos se la denomina VLAN de usuario.

Tipos de VLAN

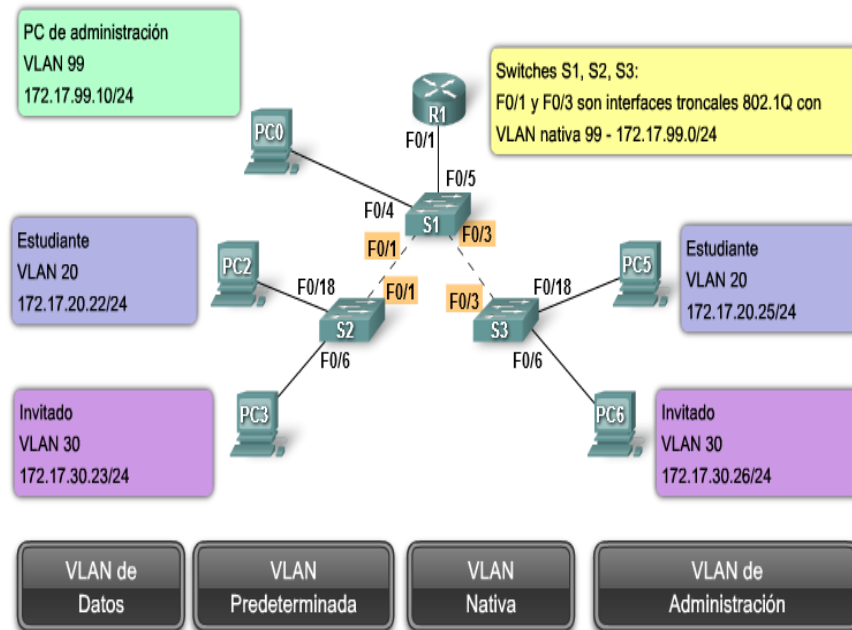


Figura 11: VLAN Predeterminada

Fuente: <http://www.cisco.netacad.net>

b. VLAN Predeterminada

Todos los puertos del switch se convierten en un miembro de la VLAN predeterminada luego del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada los hace a todos partes del mismo dominio de broadcast. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches de Cisco es la VLAN 1. La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no la puede volver a denominar y no la puede eliminar. El tráfico de control de Capa 2, como CDP y el tráfico

del protocolo spanning tree se asociará siempre con la VLAN 1: esto no se puede cambiar. En la figura, el tráfico de la VLAN1 se envía sobre los enlaces troncales de la VLAN conectando los switches S1, S2 y S3. Es una optimización de seguridad para cambiar la VLAN predeterminada a una VLAN que no sea la VLAN 1; esto implica configurar todos los puertos en el switch para que se asocien con una VLAN predeterminada que no sea la VLAN 1. Los enlaces troncales de la VLAN admiten la transmisión de tráfico desde más de una VLAN.

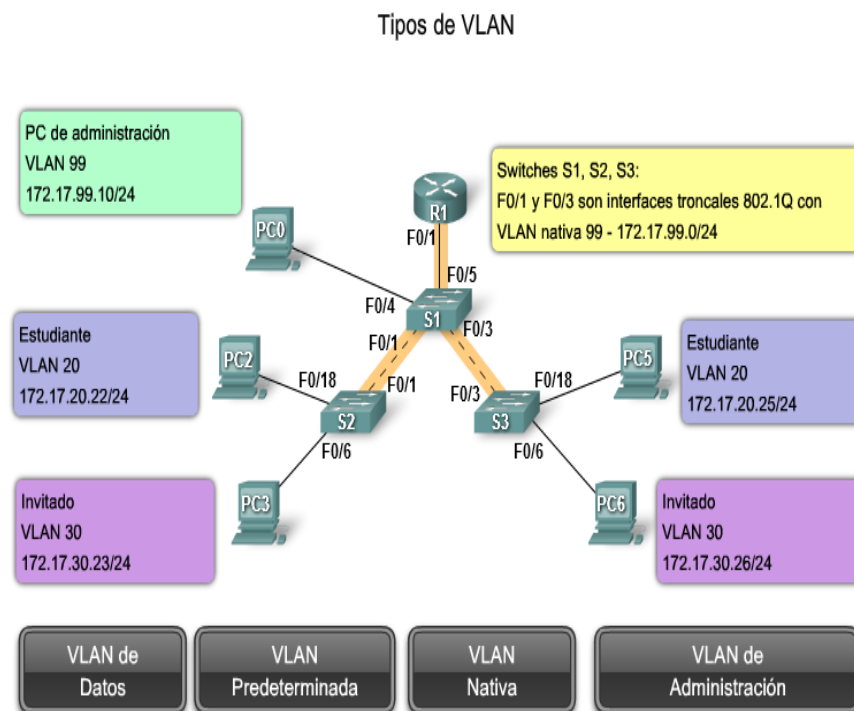


Figura 12: VLAN Nativa
Fuente: <http://www.cisco.netacad.net>

c. VLAN Nativa

Una VLAN nativa está asignada a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de

muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. En la figura, la VLAN nativa es la VLAN 99. El tráfico no etiquetado lo genera una computadora conectada a un puerto de switch que se configura con la VLAN nativa. Las VLAN se establecen en la especificación IEEE 802.1Q para mantener la compatibilidad retrospectiva con el tráfico no etiquetado común para los ejemplos de LAN antigua. Para nuestro fin, una VLAN nativa sirve como un identificador común en extremos opuestos de un enlace troncal. Es una optimización usar una VLAN diferente de la VLAN 1 como la VLAN nativa.

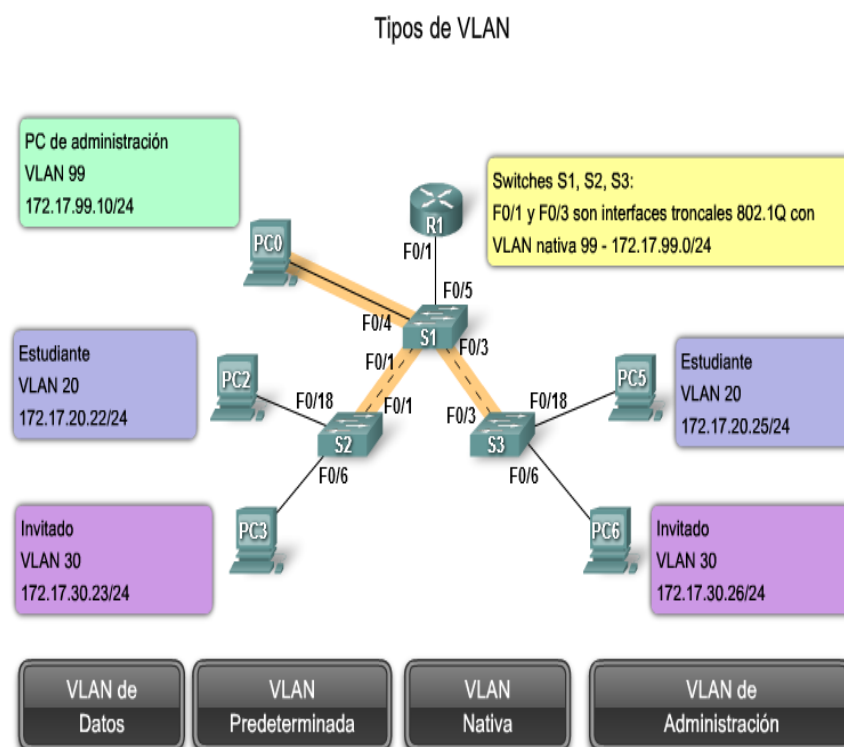


Figura 13: VLAN de Administración

Fuente: <http://www.cisco.netacad.net>

d. VLAN de Administración

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. Se asigna una dirección IP y una máscara de subred a la VLAN de administración. Se puede manejar un switch mediante HTTP, Telnet, SSH o SNMP.

e. VLAN de Voz

Es fácil apreciar por qué se necesita una VLAN separada para admitir la Voz sobre IP (VoIP). Imaginemos que estamos recibiendo una llamada de urgencia y de repente la calidad de la transmisión se distorsiona tanto que no puede comprender lo que está diciendo la persona que llama.

El tráfico de VoIP requiere:

- Prioridad de transmisión sobre los tipos de tráfico de red.
- Ancho de banda garantizado para asegurar la calidad de la voz.
- Capacidad para ser enrutado en áreas congestionadas de la red.
- Demora de menos de 150 ms a través de la red.
- Los números de acceso requieren que este introduzca el número de extensión del usuario de VoIP.
- Se requiere una cola de prioridad para VoIP.

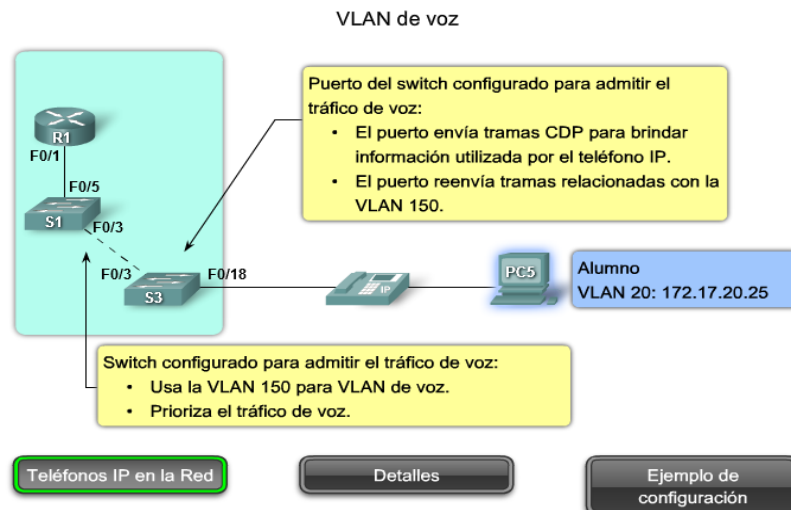


Figura 14: VLAN de Voz
Fuente: <http://www.cisco.netacad.net>

Veamos el ejemplo de la parte superior, en dicha figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC05 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes. El puerto F0/18 en S3 se configura para que esté en modo de voz a fin de que diga al teléfono que etiquete las tramas de voz con VLAN 150. Las tramas de datos que vienen a través del teléfono IP de Cisco desde la PC5 no se marcan. Los datos que se destinan a la PC5 que llegan del puerto F0/18 se etiquetan con la VLAN 20 en el camino al teléfono, que elimina la etiqueta de la VLAN antes de que los datos se envíen a la PC5. Etiquetar se refiere a la adición de bytes a un campo en la trama de datos que utiliza el switch para identificar a qué VLAN se debe enviar la trama de datos.

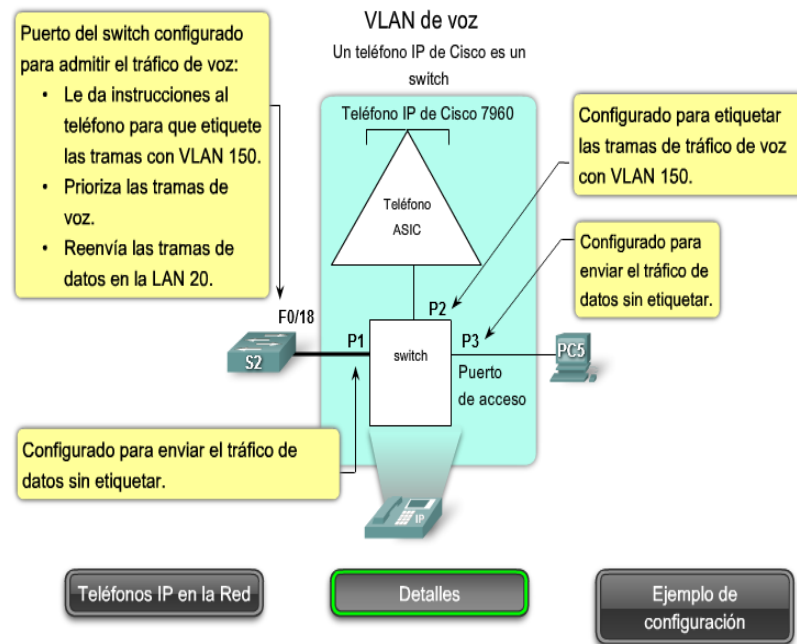


Figura 15: Como conectar un telefono IP de Cisco

Fuente: <http://www.cisco.netacad.net>

f. Teléfono IP

El teléfono IP de Cisco posee un switch integrado de tres puertos 10/100, tal como se muestra en la figura de la parte posterior. Los puertos proporcionan conexiones dedicadas para estos dispositivos:

El puerto 1 se conecta al switch o a otro dispositivo de voz sobre IP (VoIP).

El puerto 2 es una interfaz interna 10/100 que envía el tráfico del teléfono IP.

El puerto 3 (puerto de acceso) se conecta a una PC u otro dispositivo.

La función de la VLAN de voz permite que los puertos de switch envíen el tráfico de voz IP desde un teléfono IP. Cuando se

conecta el switch a un teléfono IP, el switch envía mensajes que indican al teléfono IP conectado que envíe el tráfico de voz etiquetado con el ID 150 de VLAN de voz. El tráfico de la PC conectada al teléfono IP pasa por el teléfono IP sin etiquetar. Cuando se configuró el puerto del switch con una VLAN de voz, el enlace entre el switch y el teléfono IP funciona como un enlace troncal para enviar tanto el tráfico de voz etiquetado como el tráfico de datos no etiquetado.

2.3.12.4 Métodos principales de definición de pertenencia a VLAN

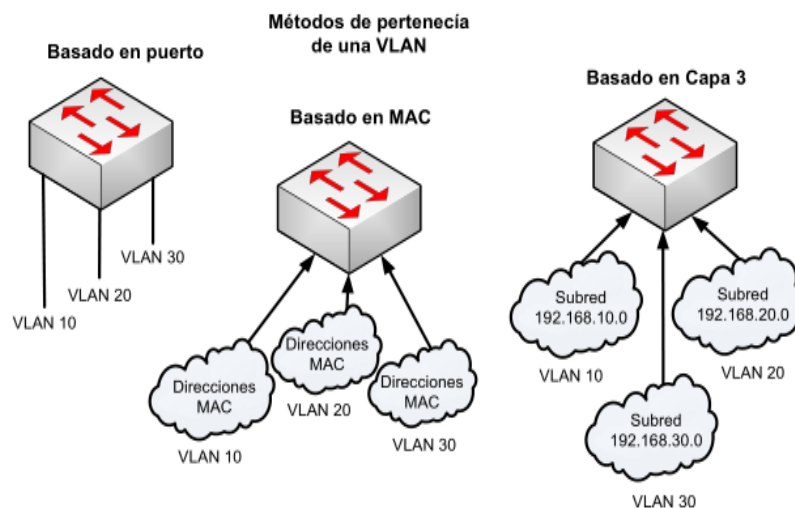
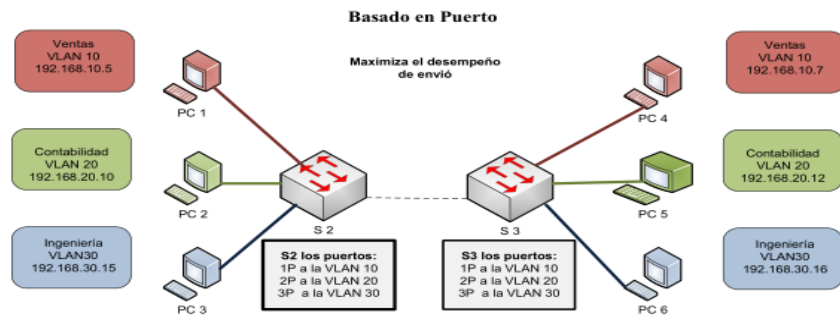


Figura 16: Métodos de pertenencia de una VLAN

Fuente: Elaboración propia

- Basado en puerto



SWITCH 1	
VLAN	PUERTOS
VLAN 10 “Ventas”	1
VLAN 20 “Contabilidad”	2
VLAN 30 “Ingeniería”	3
SWITCH 2	
VLAN	PUERTOS
VLAN 10 “Ventas”	1
VLAN 20 “Contabilidad”	2
VLAN 30 “Ingeniería”	3

Figura 17: VLAN basado en puerto

Fuente: Elaboración propia

Es el método de configuración más común. Los miembros de la VLAN se especifican en base al puerto en el cual se encuentran conectados a los dispositivos de interconexión. Los puertos se asignan individualmente a cada VLAN.

Se implementa a menudo donde el protocolo de control de host dinámico (DHCP) se usa para asignar las direcciones IP al host de red. Los paquetes no se filtran a otros dominios.

El uso es sencillo y se administran fácilmente mediante las GUI.

- Basado en dirección MAC

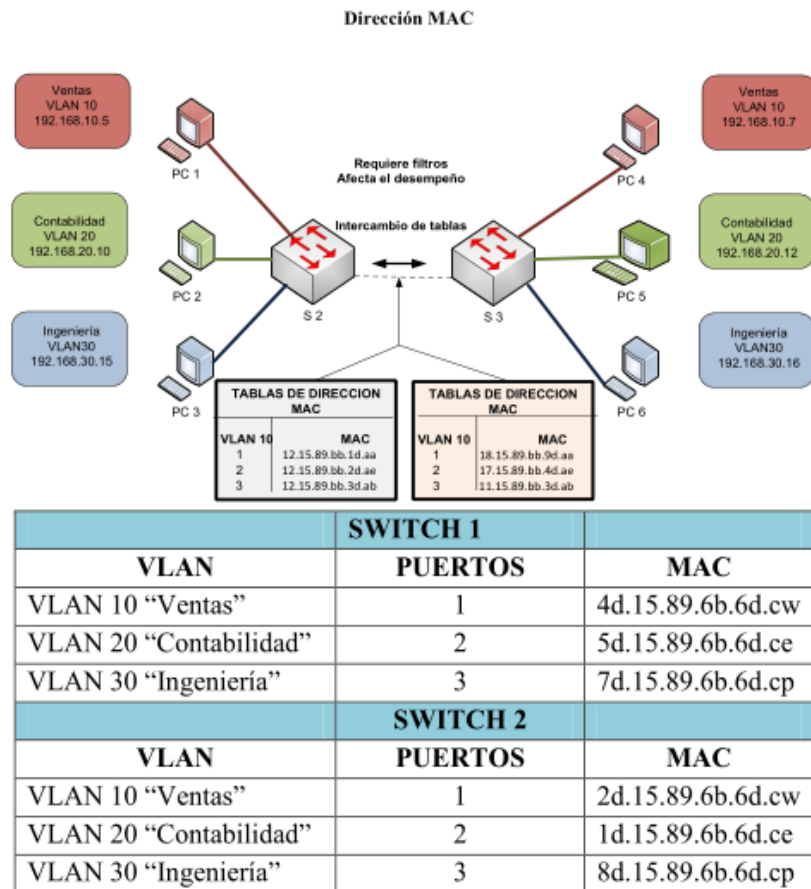


Figura 18: VLAN basado en MAC

Fuente: Elaboración propia

Este método es implementado con escasa frecuencia hoy en día. Los miembros de una VLAN dependen de la dirección MAC de las estaciones. No requiere reconfiguración si las estaciones se mueven físicamente a puertos distintos. Es necesario introducir y configurar cada dirección de forma individual inicialmente para determinar a que VLAN pertenece.

- Basado en protocolo

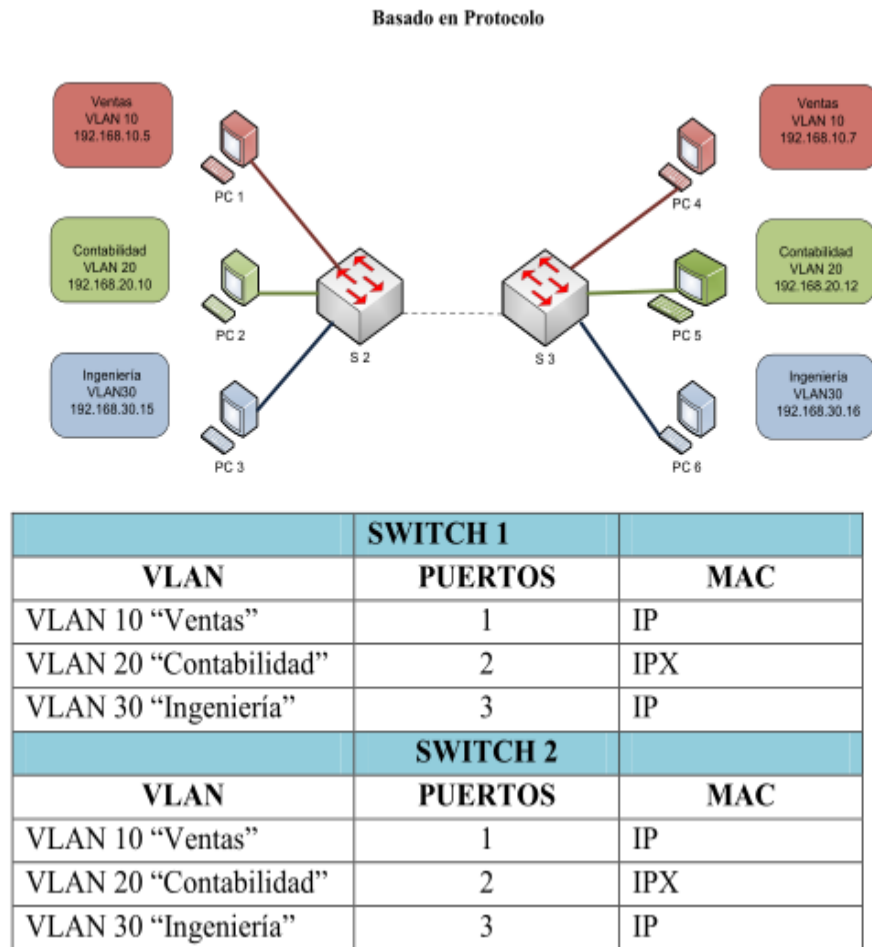


Figura 19: VLAN basado en protocolo

Fuente: Elaboración propia

Se configura con las direcciones MAC, pero usan una dirección lógica o IP. Lo que pertenezca a IP se encaminará a la VLAN de IP e IPX se dirigirá a la VLAN de IPX, es decir, se tendrá una VLAN por protocolo. Las ventajas que se obtienen con este tipo de VLAN radican en que dependiendo del protocolo que use cada usuario, este se conectará automáticamente a la VLAN correspondiente. Estas ya no son muy comunes debido a DHCP.

2.3.12.5 Protocolos que permiten la integración de las VLAN's

- **IEEE 802.1Q**

Para Carlos Valdivia (2015) es el estándar y es compatible con otros fabricantes. Es un protocolo de enlace troncal que permite interconectar un switch Cisco con otro de distinto fabricante. Este protocolo introduce el concepto de VLAN nativa, que comprende todo el tráfico sin etiqueta que entra por un puerto perteneciente a la VLAN a la que pertenecía el puerto antes de ser configurado como enlace troncal.

- **VTP**

Cisco Systems (2012) define que la VLAN “Trunk Protocol” (VTP) es un protocolo basado en mensajes “Multicast” de capa 2 desarrollado por Cisco, este protocolo provee las funciones para identificar las diferentes VLAN así como los esquemas para mantener una consistencia en la configuración de VLAN a través de la red. VTP maneja la adición, eliminación y reubicación de VLAN's en el sistema sin tener que realizarlo manualmente en cada conmutador. Este protocolo a través de mensajes “Multicast” periódicos envía y toma los mensajes y los da a conocer a otros conmutadores que conforman el dominio. VTP provee para cada conmutador la transmisión de avisos en “frames” sobre cada uno de sus puertos configurado como “Trunk”. Estos avisos son enviados en “Multicast” y son recibidos por todos los conmutadores del dominio. Este aviso contiene el dispositivo que administra el dominio, las VLAN's

que el dispositivo conoce y los parámetros para cada VLAN conocida. Al escuchar estos avisos, todos los dispositivos que están en el mismo dominio de administración aprenden alguna nueva VLAN que se haya configurado. Usando este método una VLAN solo es necesario crearla o configurarla una sola vez en el dominio de administración y la información automáticamente es aprendida por todos los demás dispositivos que conforman el dominio. Por ejemplo, cuando un nuevo conmutador es agregado a la red, éste recibe notificaciones VTP y es automáticamente configurado para manejar las VLAN's existentes dentro de la red.

2.3.13 Metodología Cisco

Dentro de la metodología Cisco existe una metodología de fase de diseño denominada: “**Top-down**”. Veamos sus fases:

- **Fase 1: Analizar Requisitos**

En esta fase se realizan entrevistas con usuarios y personal técnico, se analizan metas de negocio, restricciones, sesgos, metas técnicas, balances, restricciones y por último caracterizar la red existente (rendimiento actual).

- **Fase 2: Diseño Lógico de Red**

Es la fase donde se diseña la topología de la red, se realiza la selección de protocolos de conmutación (switching) con enrutamiento (routing) y se desarrolla estrategias para la seguridad y mantenimiento de la red.

- **Fase 3: Diseño Físico de Red**

Esta fase se utiliza para seleccionar las tecnologías y dispositivos para la(s) red(es).

- **Fase 4: Probar, Optimizar y Documentar el diseño de red**

En esta fase se prueba, optimiza y documenta los diseños de la red.

2.3.14 Herramienta de Simulación

2.3.14.1 Simulación

La simulación es la imitación del funcionamiento de un sistema real durante un intervalo de tiempo. Actualmente las herramientas de simulación son de gran utilidad debido a que se puede prever el comportamiento de un sistema y/o topología antes de implementarlo, se pueden encontrar comportamientos del sistema que no se detectan fácilmente por la complejidad del estudio y una razón muy importante en cualquier empresa es el ahorro de dinero porque ayuda al diseño y perfeccionamiento del sistema y/o topología a construir.

2.3.14.2 Cisco Packet Tracer

Es un software que permite crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Se enfoca en apoyar mejor los protocolos de red.

Hoy en día, es la herramienta de simulación más utilizada, conforme los productos de la Familia Cisco van ganando terreno en el mercado de equipos orientados al soporte de la Plataforma de Red. Soporta los siguientes protocolos:

- HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP y DNS.
- TCPIUDP, 1Pv4, 1Pv6, ICMPv4 e ICMPv6.
- RIP, EIGRP, OSPF Multitarea, enrutamiento estático y redistribución de rutas.
- Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP, ARP, CDP, STP, RSTP, 802.1q, VTP, DTP y PAgP, Polly Mkt.

CAPÍTULO 3: METODOLOGÍA Y DISEÑO DE LA INVESTIGACIÓN

3.1 Clase y diseño de investigación

3.1.1 Clase de investigación

Viendo los objetivos y la hipótesis, se denomina a este tipo de investigación “proyectiva”.

Según Hurtado (2008), “El tipo de investigación proyectiva consiste en la elaboración de una propuesta un plan, un programa o un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, o de una región geográfica, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y de las tendencias futuras, es decir, con base en los resultados de un proceso investigativo.

3.1.2 Diseño de investigación

El diseño es **no experimental** porque según Kerlinger & Lee (2002) no se posee control directo de las variables independientes debido a que sus manifestaciones ya han ocurrido o no son manipulables. Se hacen inferencias sobre relaciones entre variables, sin intervención directa.

3.2 Población de investigación

Población:

Usuarios con acceso a la red de área local del Hospital III José Cayetano Heredia, los cuales se cuantifican hasta el momento un total de 110 personas.

Muestra:

La muestra no probabilística son los usuarios de se encuentran en los departamentos en mención con acceso a la red del área local del Hospital III José Cayetano Heredia.

3.3 Ubicación y descripción de la población

La sede central del Hospital III José Cayetano Heredia se encuentra ubicada en la ciudad Av. Independencia S/N Castilla, Piura.

3.4 Técnicas e instrumentos para obtener datos

Las técnicas utilizadas para la recolección de datos serán la encuesta y la observación, por lo mismo el instrumento para la recolección de datos será el cuestionario (**ANEXO 9**) y sus resultados (**ANEXO 10**).

Se ha considerado el uso de guía de observación N° 1 (**ANEXO 11**) debido a que se debe medir velocidad de tráfico y demás indicadores que no se podrían medir mediante preguntas.

Además de los resultados de la guía de observación (**ANEXO 12**).

3.5 Metodología para el procesamiento y análisis de datos

Los métodos de análisis de datos serán estadísticos, determinando tablas de frecuencia y las medidas de tendencia central, así como gráficos de histograma. El procesamiento se realizará en Excel y el software de Estadística SPSS.

Tabla 8 - Técnicas e Instrumentos

Indicador	Descripción	Técnica	Instrumento	Informante
I N° 1	Velocidad de Tráfico	Observación	Guía de Observación N° 1	Personal de la institución.
I N° 2	Incremento de Seguridad	Encuesta	Cuestionario N° 1	Personal de la institución.
I N° 3	Cableado estructurado acorde a estándares internacionales	Observación	Guía de Observación N° 1	Personal de la institución.

Elaboración: Propia

CAPÍTULO 4: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN

4.1 Análisis del estado actual de la red

De acuerdo a Cisco Systems y Oppenheimer (2011), Top-Down Network Design, 3era edición, United State of America; Cisco Press, se llevó a cabo el análisis de red.

4.2 Metas del diseño de red

- Reducir los problemas de conexión.
- Elevar la productividad de los usuarios.
- Gestionar el uso eficiente de los sistemas informáticos y/o las TIC.
- Asegurar el acceso a la información.

4.3 Metas técnicas

- Rediseño del direccionamiento IP.
- Brindar seguridad a los usuarios que acceden a la red.
- Proveer seguridad para proteger conexiones a la red.
- Brindar una red escalable.
- Priorizar el tráfico de red.

4.4 Ámbito

El proyecto comprende el análisis, entendimiento de la arquitectura y rendimiento de la red del Hospital III José Cayetano Heredia, que comprende los siguientes departamentos:

- División Soporte Informático
- Dosis Unitaria
- Instituto Peruano de Oftalmología (IPO)

- Historias Clínicas
- Control Tiempo
- Cuerpo Médico
- Centro de Prevención de Riesgo del Trabajo (CEPRIT)
- Prestaciones Económicas
- Asesoría Jurídica
- Banco de Sangre
- EsSalud en línea
- Consultorios
- Caja Facturación

4.5 Restricciones

Dado que el proyecto simulará una nueva topología de red utilizando VLANs, no existen gastos en equipos, licencias, servicios de mantenimiento u otros. No obstante, la finalidad de esta propuesta es que quede registrado como evidencia que en mediano o largo plazo se pueda implementar el modelo propuesto en el trabajo de investigación.

4.6 Uso actual de la red

Tabla 9 - Usuarios por área

ITEM	ÁREA	USUARIOS
1	División Soporte Informático	10
2	Dosis Unitaria	9
3	Instituto Peruano de Oftalmología (IPO)	6

4	Historias Clínicas	9
5	Control Tiempo	6
6	Cuerpo Médico	10
7	Centro de Prevención de Riesgo del Trabajo (CEPRIT)	10
8	Prestaciones Económicas	9
9	Asesoría Jurídica	6
10	Banco de Sangre	9
11	EsSalud en línea	6
12	Consultorios	10
13	Caja Facturación	10

Elaboración: Propia

Tabla 10 - Anexos Telefónicos por área

ITEM	ÁREA	USUARIOS
1	División Soporte Informático	10
2	Dosis Unitaria	9
3	Instituto Peruano de Oftalmología (IPO)	6
4	Historias Clínicas	9
5	Control Tiempo	6
6	Cuerpo Médico	10
7	Centro de Prevención de Riesgo del Trabajo (CEPRIT)	10
8	Prestaciones Económicas	9
9	Asesoría Jurídica	6
10	Banco de Sangre	9

11	EsSalud en línea	5
12	Consultorios	10
13	Caja Facturación	10

Elaboración: Propia

Tabla 11 - Interfaces de red disponibles

Switches en funcionamiento	13
Total de Puertos de los switches	312
Puertos Disponibles no utilizados por usuarios, teléfonos y enlace entre switches	80

Elaboración: Propia

4.7 Direcciones IP disponibles

Segmento de red utilizado:

Red: 192.168.1.0

Mascara:

255.255.255.0

Tabla 12: Direcciones IP – Red actual

Número de direcciones IP utilizadas	232
Número de direcciones IP disponibles	80

Elaboración: Propia

4.8 Rendimiento de la red

El Jefe encargado de la red asistencial indica que se debe trabajar sin inconvenientes por parte de los usuarios, el mismo no especifica cual es la performance de la red.

Para establecer las metas de performance se tomó en cuenta los siguientes factores:

Ancho de banda (bps)

Hoy en día, el hospital cuenta con un plan de internet, veamos a detalle:

Tabla 13: Ancho de banda contratado

Ítem	Plan de internet contratado	Ancho de banda
01	Linea Dedicada	4Mbps

Fuente: Departamento de Soporte Informático

Elaboración: Propia

Las interfaces de red ethernet de los equipos como routers, switches y el medio de conexión corren a 10Mbps y 100Mbps.

4.9 Latencia

Es un indicador muy significativo. Se mide a través de PING, para hacer ping a toda la red se utilizó MS-DOS.

4.10 Seguridad

Riesgos de seguridad

A continuación, se muestran algunas amenazas a la red:

Tabla 14: Activos de red - Amenazas de seguridad

Ítem	Amenazas	Probabilidad
01	Infiltración de usuarios no autorizados en la red	Muy alta
02	Robo de información	Muy alta
03	Uso no autorizado de software y/o hardware	Muy alta
04	Uso indebido de banda ancha	Muy alta
05	Configuración de equipos sin autorización	Baja

**Fuente:
de Soporte
Elaboración:**

**Departamento
Informático
Propia**

4.11

06	Manipulación de equipos de red sin autorización	Media
07	No evaluar riesgos periódicamente	Alta

Infraestructura de red

La red del hospital III José Cayetano Heredia es una red cableada que cuenta con un switch **CORE** marca **Cisco** modelo **Catalyst** serie **4506-E** (**ANEXO 5**) que es aquel que provee alta velocidad y debe manejar los paquetes tan rápido como sea posible ya que es el cerebro de la red. Se encuentra en el Departamento de Soporte Informático y que es el corazón de la red.

A la vez, existen múltiples switches de la marca **Alcatel Lucent** modelo **OmniStack** serie **LS 6224P** de 24 puertos Fast Ethernet (**ANEXO 6**), las cuales están distribuidas en todo el largo y ancho del hospital en los diferentes departamentos con la finalidad de generar comunicación de capa 2 sobre dispositivos finales.

Los switches están conectados con cable UTP, los mismos que están guiados por canaletas que siguen un canal con puntos RJ45 categoría 5.

Los departamentos cuentan con teléfonos IP marca Yealink modelo SIP-T23G (**ANEXO 7**).

Solo el personal que se encuentra en el nivel estratégico cuenta con un teléfono IP de la misma marca Yealink modelo SIP-T48G (**ANEXO 8**) con panel función táctil, como es el caso de Gerencia y los Jefes.

La red presenta una topología estrella, con un diseño físico plano, lo cual representa demasiadas desventajas, incluyendo un único dominio de broadcast de capa 2 como, por ejemplo, una petición ARP, viaja hacia cada uno de los hosts y dispositivos en la

red LAN. Estos y otros broadcasts de capa 2 consumen una gran cantidad de ancho de banda disponible de la red LAN, adicionalmente el volumen de información que se origina entre los hosts durante horas genera los famosos “cuellos de botella”.

La asignación de IP’s en cada PC es manual, su diseño lógico ofrece una menor flexibilidad en el tráfico de red.

Las características técnicas de los dispositivos de conectividad son de nivel bajo, como es el caso de los switches, que no poseen la capacidad suficiente para soportar las altas exigencias que hoy en día tolera la red.

El cableado estructurado no esta implementado de acuerdo a las normas de calidad, respetando así espacios entre distintos enlaces, canaletas correctamente ubicadas, etc.

Veamos la comunidad de usuarios distribuidos en el hospital III José Cayetano Heredia:

Tabla 15: Switch por agrupación de usuarios

Planta	Departamentos	Número de switch	Total
--------	---------------	------------------	-------

Primera	División Soporte Informático, Dosis Unitaria, IPO, Historias Clínicas, Control Tiempo, Cuerpo Médico, CEPRIT	1	7
Segunda	Prestaciones Económicas, Asesoría Jurídica, Banco de Sangre, EsSalud en Línea, Consultorios, Caja Facturación	1	6

Elaboración: Propia

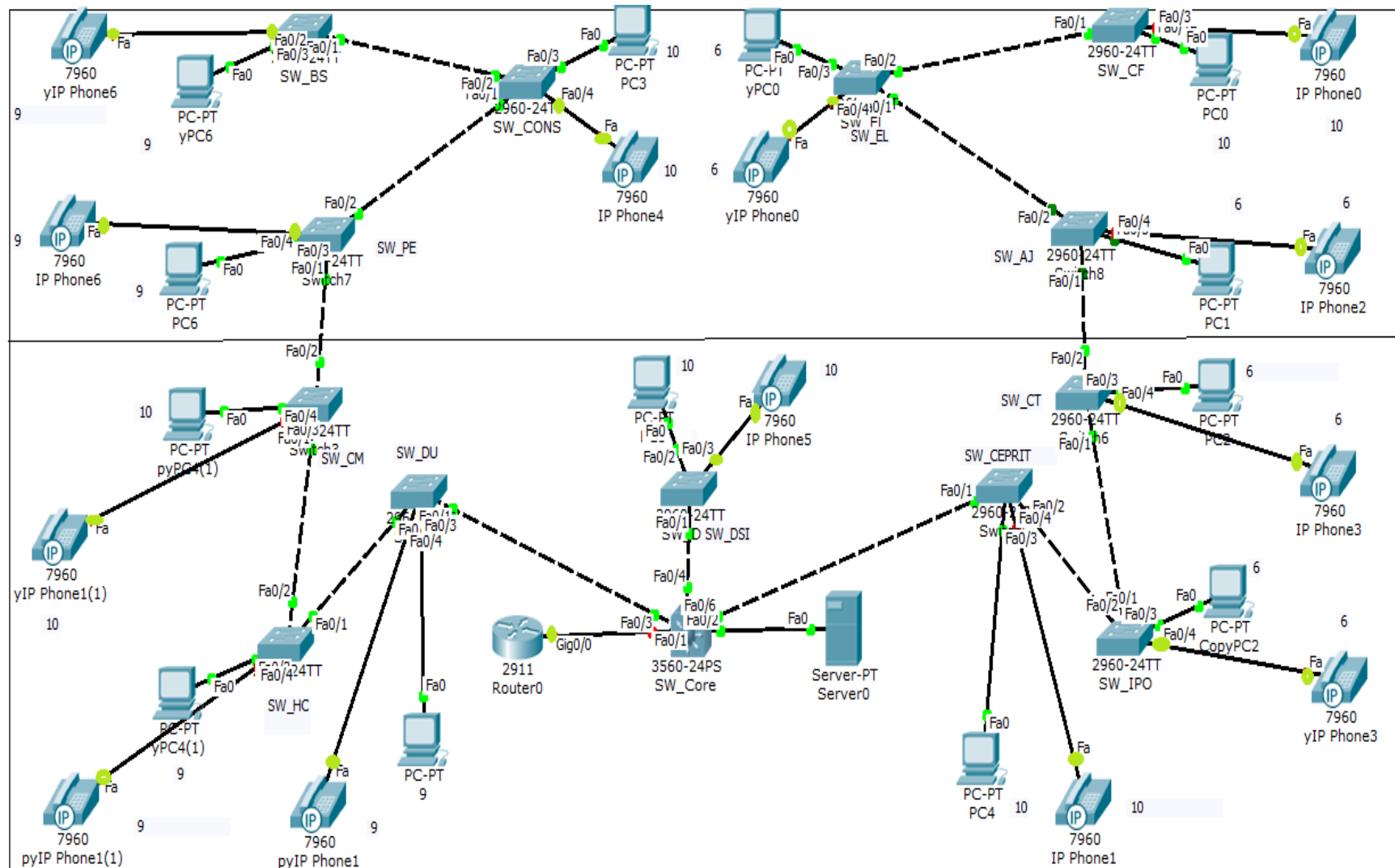


Figura 20: Red Actual del Hospital III José Cayetano Heredia

Fuente: Departamento de Soporte Informático

Como se precisa, el departamento de Soporte Informático no cuenta con registros de usuarios.

Tecnologías utilizadas

Las tecnologías LAN funcionan de la siguiente manera:

- Fast Ethernet 100Mbps
- Ethernet 10Mbps

Cableado utilizado

El cableado vertical y el cableado backbone tienen las siguientes características:

- Cobre: UTP categoría 5
- Distancia máxima: 40m
- Conector: RJ45

4.12 Diseño del modelo

4.12.1 Diseño lógico propuesto y topología de red

Jerarquía de diseño

Según los parámetros establecidos para el diseño de redes Top-Down se consideran las siguientes áreas correspondientes como nuestro planteamiento:

- Central de Datos: aquí, se ubicarán el switch Core, servidor, switches y Teléfonos IP del primer nivel.
- En el segundo nivel se ubicarán los swiches del segundo nivel.
- LAN: contará con el cableado respectivo y con dispositivos finales.

Ahora, veamos la nueva topología propuesta:

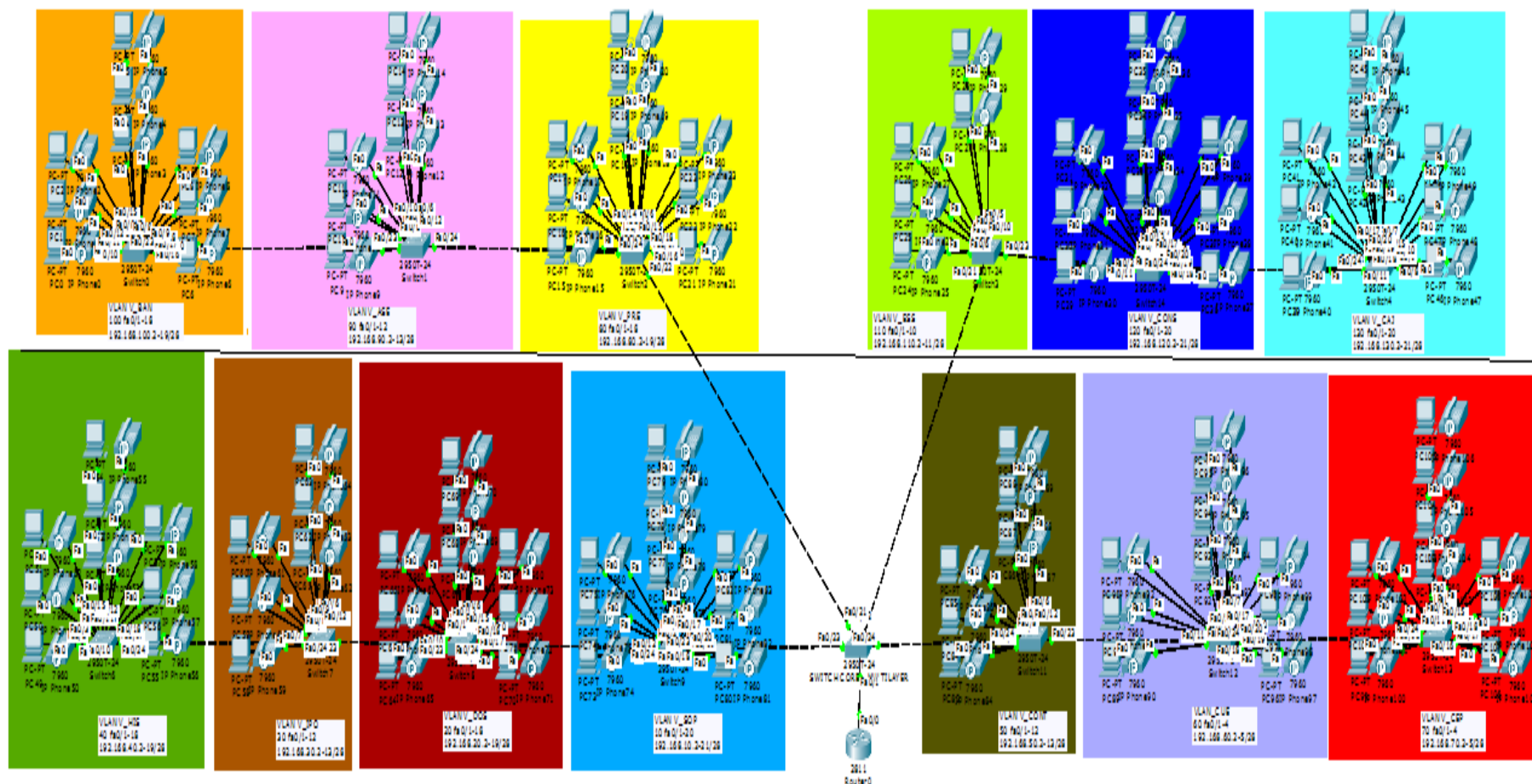


Figura 21: Topología de red propuesta basada en VLANs
Elaboración: Propia

4.12.2 Creación de VLANs

Para la simulación de la creación de VLANs, se utilizarán los Departamentos donde se encuentre ubicado un switch. La

Las creaciones de las mismas se muestran en el (**ANEXO 13**)

4.12.3 Estructura del modelo según RFC

Según el manifiesto al documento RFC 1918 que subscribe “Mejores prácticas actuales” para el direccionamiento, se permite el uso del bloque de las direcciones privadas clase C.

Red a emplear: 192.168.0.0

Tabla 16: Modelo de direccionamiento IP

192	168	0	0
Bloque 1	Bloque 2	Bloque 3	Bloque 4

Elaboración: Propia

Bloque 1 y 2 son prefijos de red clase C, son valores únicos 192.168.

Bloque 3: Identificador de comunidad de usuarios, su cantidad máxima de comunidades es 256.

Las comunidades son las siguientes:

- 10: Soporte Informático
- 20: Dosis unitaria
- 30: IPO
- 40: Historias Clinicas
- 50: Control Tiempo
- 60: Cuerpo médico
- 70: CEPRIIT
- 80: Prestaciones económicas

- 90: Asesoría Jurídica
- 100: Banco de sangre
- 110: EsSalud en línea
- 120: Consultorios
- 130: Caja Facturación
- 140: Teléfonos IP

Bloque 4: Identificador de host

- Número máximo de host: 254

Segmentos detallados: Veamos la cantidad de usuarios por cada subred.

Tabla 17: Número de usuarios por comunidad que tendrán VLAN

VLAN	Dirección / Oficina	Usuarios
10	Soporte Informático	10
20	Dosis Unitaria	9
30	IPO	6
40	Historias Clínicas	9
50	Control Tiempo	6
60	Cuerpo Médico	10
70	CEPRIT	10
80	Prst económicas	9
90	Asesoría Jurídica	6

Elaboración: Propia

4.12.4 VLAN

Por
asignó
y

100	Banco de sangre	9
110	EsSalud en línea	5
120	Consultorios	10
130	Caja Facturación	10
140	Telefonos	109

cada subred, se
una VLAN de datos
VLAN de VoIP
respectivamente.

Veamos a detalle los usuarios con sus respectivas VLANs.

Tabla 18: Comunidad de usuarios – VLANs – Dirección IP

Item	Oficina	Usu	Max. Usu	Nombre de VLAN	ID de VLAN	Dirección de red
1	Soporte Informático	10	14	V_SOP	10	192.168.10.0/28
2	Dosis Unitaria	9	14	V_DOS	20	192.168.20.0/28
3	IPO	6	14	V_IPO	30	192.168.30.0/28
4	Historias Clínicas	9	14	V_HIS	40	192.168.40.0/28
5	Control Tiempo	6	14	V_CONT	50	192.168.50.0/28
6	Cuerpo Médico	10	14	V_CUE	60	192.168.60.0/28
7	CEPRIT	10	14	V_CEP	70	192.168.70.0/28
8	Prestaciones Económicas	9	14	V_PRE	80	192.168.80.0/28
9	Asesoría Jurídica	6	14	V_ASE	90	192.168.90.0/28
10	Banco de sangre	9	14	V_BAN	100	192.168.100.0/28
11	EsSalud en Línea	5	14	V_ESS	110	192.168.110.0/28
12	Consultorios	10	14	V_CONS	120	192.168.120.0/28
13	Caja Facturación	10	14	V_CAJ	130	192.168.130.0/28

14	Teléfono IP	109	126	V_VOIP	140	192.168.140.0/25
----	-------------	-----	-----	--------	-----	------------------

Elaboración: Propia

4.12.5 Dispositivos

Tecnología

LAN

- Gigabit Ethernet BaseT
- Fast Ethernet BaseT

Características

Veamos las características de los equipos de red:

Equipo de Distribución: Router Cisco 2911

- Interfaces: Tres (03) puertos gigabit full dúplex con conector es RJ45, dos puertos de consola RJ45, un puerto USB mini y dos puertos serial.
- Memoria RAM de 512 MB por defecto, se puede remontar a 2 GB.
- Memoria Flash de 256 MB ampliable a 4GB.

Equipo de Acceso: Cisco Catalyst 2960-X Series

- Interfaces: Veinticuatro (24) puertos FastEthernet con soporte PoE, dos (02) puertos Gigabit Ethernet, ambos cuentan con conectores RJ45 full duplex.
- Memoria RAM de 512 MB.
- Memoria Flash de 128 MB.

Veamos la lista de equipos en un cuadro resumen.

Tabla 19: Equipos de red

Capa	Equipo	Cantidad	Puertos	Adm
Core - Distribución	Router Cisco 2911	01	03	Sí
Acceso	Switch Cisco Catalyst 2960- X Series	13	24	Sí

Elaboración: Propia

4.12.6 Configuración de equipos

La configuración de los equipos de red en modo simulación se llevó a cabo mediante la interface de línea de comando de Cisco (CLI), la cual se puede ver con más detalle en la simulación cuando se exponga el proyecto. (**ANEXO 14**)

4.13 Simulación y evaluación del modelo propuesto

4.13.1 Simulación y evaluación

Se utilizó el simulador de redes Packet Tracer de Cisco, se simuló el modelo y se logró lo siguiente:

Escalabilidad

Debido al modelo de tres capas de Cisco, la escalabilidad se puede implementar de manera sencilla sin afectar el rendimiento de la red.

Plan de expansión

Lo que se obtuvo del análisis, se proyecta el crecimiento en cada comunidad de usuarios.

Ancho de banda

Los dispositivos de red propuestos soportan 100 y 1000 Mbps (FastEthernet y GigabitEthernet).

	RED ACTUAL	RED NUEVA
VELOCIDAD DE TRÁFICO	100 Mbps	1000 Mbps
INCREMENTO DE SEGURIDAD	INSEGURO	MUY SEGURO
CABLEADO ESTRUCTURADO ACORDE A ESTÁNDARES INTERNACIONALES	NO CUMPLE	SÍ CUMPLE

Elaboración: Propia

CONCLUSIONES

- Se obtuvo una mejora en la velocidad del tráfico a partir de la utilización de VLANs.
- Hubo un incremento de seguridad de la información que se transfiere y comparte en la red.
- Se obtuvo mejoras en la implementación del cableado estructurado acorde a lo establecido por estándares internacionales.
- En la propuesta de red se reduce significativamente la latencia.

SUGERENCIAS

- Implementar el modelo siguiendo detalladamente los pasos indicados, con el objetivo de mejorar el rendimiento y a la vez cumplir con los objetivos institucionales del Hospital III José Cayetano Heredia.
- Se sugiere considerar para su respectiva revisión el modelo antes de realizar gastos en compra de equipos o contratación de servicios relacionados a la red de datos.
- Una vez expuesto el modelo, se sugiere al Departamento de Soporte Informático hacer el uso adecuado de la nueva red e innovar con la comunicación rápida y segura vía video conferencias.
- A los futuros tesisistas, se sugiere utilizar herramientas que permitan analizar el tráfico de red de manera individual, es decir el que genera cada usuario de la red de datos, esto para sustentar cambios en la configuración base.

BIBLIOGRAFÍA

ATELIN, P., & DORDOIGNE, J, Redes informáticas: conceptos fundamentales: normas, arquitectura, modelo OSI, TCP/IP, Ethernet, Wi-Fi. Ediciones ENI, 2006. ISBN 9782746034822.

CISCO, Internetworking Technology Handbook. Editor John Kane, 2006. ISBN 9781578701025.

HERRERA PEREZ, Tecnologías y redes de transmisión de datos. Editorial LIMUSA, 2003. ISBN 9789681863838.

ÍÑIGO GRIERA, J., BARCELÓ ORDINAS, J. M., CERDÀ ALABERN, L., PEIG OLIVÉ, E., ABELLA I FUENTES, J., & CORRAL I TORRUELLA, G, Estructuras de redes de computadores. Editorial UOC, 2009. ISBN 9788497074292.

MEJÍA MESA, A, Guía práctica para manejar y reparar el computador. Editorial Ditel Ltda, 2005. ISBN 9789589744604.

OPPENHEIMER, P. Top-down network design. Editorial Pearson Education, 2004. ISBN 9781578700691.

STALLINGS, W. Comunicacion y redes de computadoras. Editorial Pearson Education, 2000. ISBN 9788483227589.

ANEXOS

ANEXO 1 EVIDENCIAS DE LA RED ACTUAL

INFORME N° 001 - DSI-2017

A : Ing. Luis Alonso Cevallos López
Jefe División de Soporte Informático

DE : Bach. Frank García Espinoza
Ex Practicante – División Soporte Informático

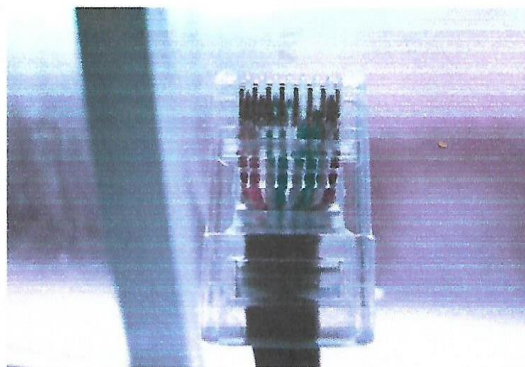
ASUNTO : Informe para el Proyecto de Investigación respecto a cableado estructurado y switch del Hospital III José Cayetano Heredia

FECHA : 28 de setiembre del 2017

Me dirijo a Ud., para saludarlo cordialmente y en relación al Proyecto de Investigación se informa lo siguiente:

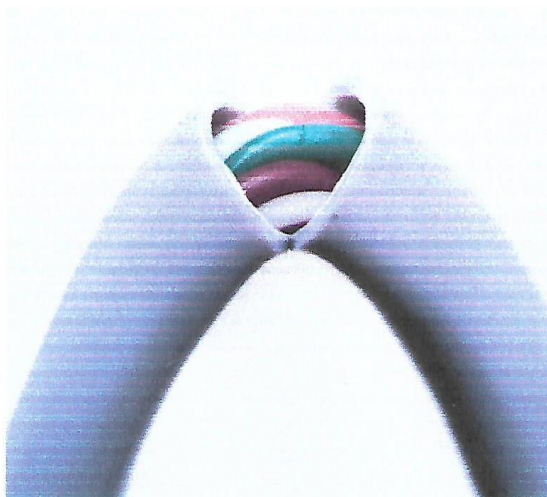
1. Alcance del cableado estructurado:

Como parte del Sistema de Cableado estructurado se evidencia que los hilos 5 y 6 no van por su carril (fallan dos conexiones). Además, el conector RJ45 y el cable UTP está mal crimpado.



Fuente: División Soporte Informático – Red Asistencial Piura

Existen cables UTP con aberturas en su funda. Y esto suele ocurrir porque no las canalizan con canaletas que estén compuestas por base y tapa garantizando una ruta perfecta para todos los cables, cumpliendo estándares de TIA/EIA 568A y 569A

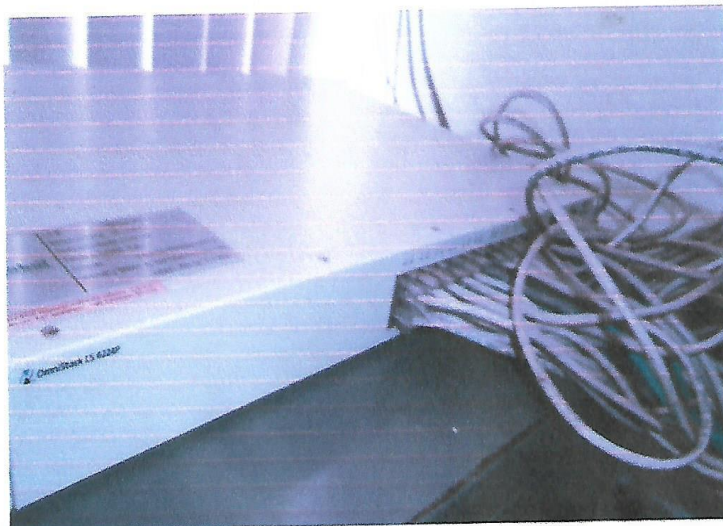


Fuente: División Soporte Informático – Red Asistencial Piura

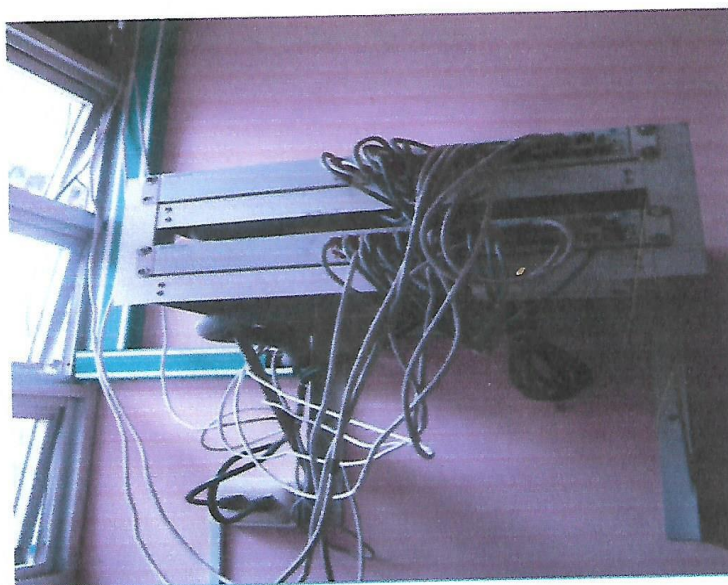
2. Alcance de los switches:

Se recopiló información del estado actual en el que se encuentran los switches de la red actual del Hospital III José Cayetano Heredia evidenciando los siguientes aspectos:

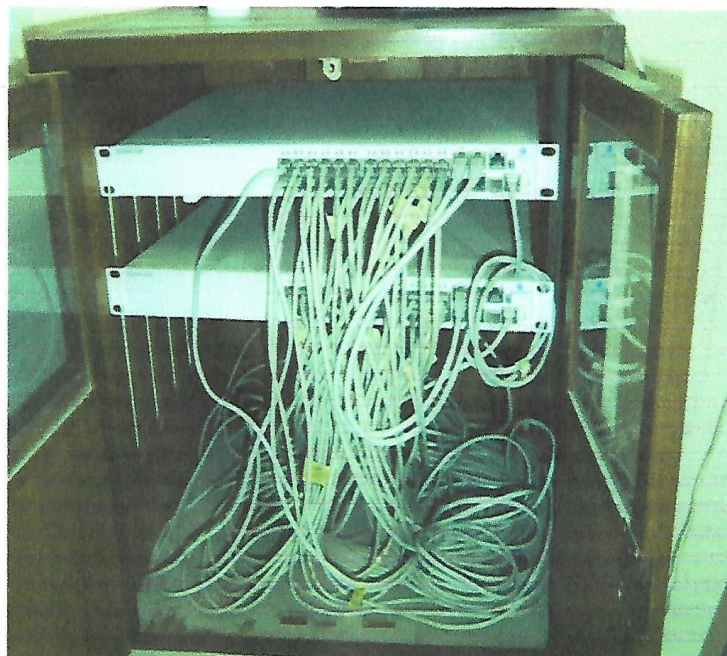
- a) Cableado montado y sin canalizar.
- b) Un switch encima de otro switch
- c) Espacio cerrado y sin ventilación
- d) Cableado amarrado por cinta aislante
- e) Bandejas de canaletas abiertas por las tapas
- f) Cableado expuesto a los rayos del sol



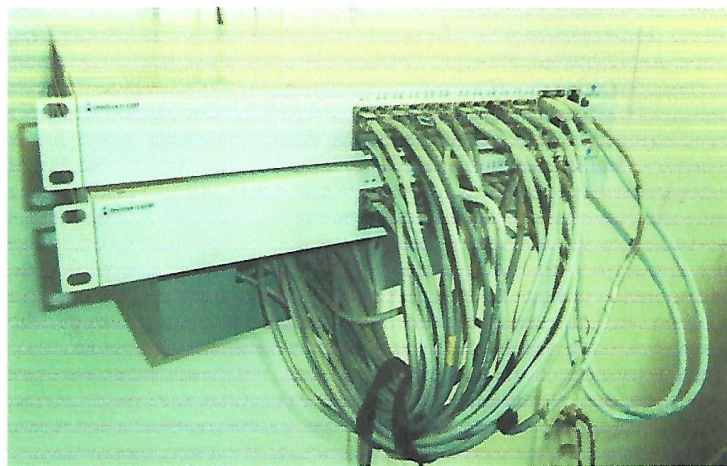
Fuente: División Soporte Informático – Red Asistencial Piura



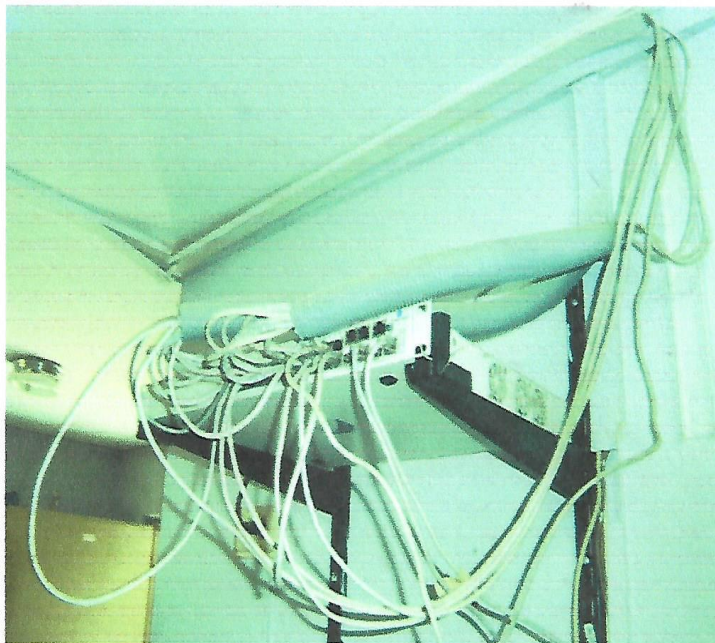
Fuente: División Soporte Informático – Red Asistencial Piura



Fuente: División Soporte Informático – Red Asistencial Piura



Fuente: División Soporte Informático – Red Asistencial Piura



Fuente: División Soporte Informático – Red Asistencial Piura



Fuente: División Soporte Informático – Red Asistencial Piura


Esto todo cuanto tengo que informar, para los fines correspondientes, salvo mejor parecer de su despacho.

Atte,

Atentamente.



Luis Alonso Cevallos Lopez
REG. CIP 221254
JEFE DE DIVISION SOPORTE INFORMATICO
RED ASISTENCIAL PIURA



Bach. Frank Garcia Espinoza
Ex practicante - División Soporte
Informático
Red Asistencial Piura

ANEXO 2 ANÁLISIS ECONÓMICO

a) Mano de Obra

ITEM	DESCRIPCIÓN	CANTIDAD	COSTO DIA	DIAS	TOTAL
1	Técnico en cableado de redes	3	S/. 120.00	14	S/. 1,680.00
2	Supervisor de cableado Estructurado	1	S/. 180.00	14	S/. 2,520.00
3	Especialista CCNA	1	S/. 300.00	7	S/. 2,100.00
SUB TOTAL					S/. 6,300.00

Fuente: Elaboración propia

b) Materiales y Equipos

ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNIT.	SUB TOTAL
1	Router - CISCO 2811 Security Bundle, Adv Security, 128F/512D	1	S/. 4,851.46	S/. 4,851.46
2	Switch - WS-C2960X-24PS-L	13	S/. 3,301.06	S/. 42,913.78
3	Cable UTP Cat. 6	1	S/. 300.00	S/. 300.00
4	Conectores RJ45 Cat. 6 con Protector	300	S/. 2.00	S/. 600.00
5	Caja de Paso 20x20	20	S/. 20.00	S/. 400.00
6	Tapa Flex para RJ45	100	S/. 6.00	S/. 600.00
7	Conector Jack RJ45 Cat. 6	200	S/. 2.00	S/. 400.00
8	Caja Plastica sobrepuesta	100	S/. 6.00	S/. 600.00
9	Canaletas de 5" autoadhesivas	100	S/. 12.00	S/. 1,200.00
10	Canaletas de codo autoadhesivas	30	S/. 10.00	S/. 300.00
11	Etiquetas para cableado estructurado	0.5	S/. 300.00	S/. 150.00
12	Cintillos de 12x20	10	S/. 7.50	S/. 75.00
13	Otros materiales (tornillos, pegamento, etc)	1	S/. 400.00	S/. 400.00
SUB TOTAL				S/. 52,790.24

Fuente: Elaboración propia

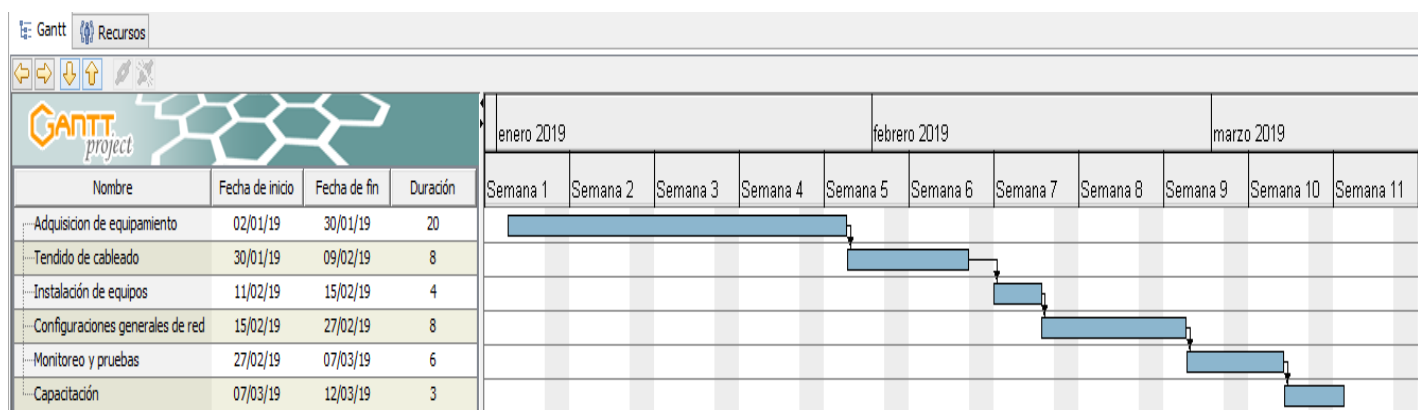
c) Resumen

ITEM	DESCRIPCIÓN	TOTAL
1	Mano de Obra	S/. 6,300.00
2	Materiales y Equipos	S/. 52,790.24
SUB TOTAL		S/. 59,090.24

Fuente: Elaboración propia

ANEXO 3

CRONOGRAMA DE ACTIVIDADES



ANEXO 4

INFORME EMITIDO POR EL RESPONSABLE DE LA RED



PERÚ

Ministerio
de Trabajo
y Promoción del Empleo

Seguro Social de Salud
EsSalud

Red Asistencial Piura



"Año del buen servicio al ciudadano"
"Año de la Lucha contra la corrupción"

CONSTANCIA

A solicitud presentada por el Sr. **FRANK GARCIA ESPINOZA**, bachiller en **INGENIERÍA INFORMÁTICA** de la **UNIVERSIDAD NACIONAL DE PIURA** identificado con DNI N° **72744754**, solicitando un informe de nuestra **RED DE DATOS** en el Establecimiento de Salud: **HOSPITAL III JOSÉ CAYETANO HEREDIA – CASTILLA, PIURA** por motivo de su Proyecto de Tesis denominado **"PROYECTO DE REDISEÑO DE RED DE COMPUTADORAS DEL HOSPITAL III JOSÉ CAYETANO HEREDIA UTILIZANDO VLANS"** se deja **CONSTANCIA** que se le ha autorizado el acceso a nuestras instalaciones y se le ha brindado la información suficiente para la elaboración de su proyecto de investigación.

En nombre del Departamento de División de Soporte Informático, damos **conformidad** al Proyecto de Investigación

Piura, 28 de Setiembre del 2017



Luis Alonso Cevallos López
REG. CIP: 131294
JEFE DE DIVISION SOPORTE INFORMATICO
RED ASISTENCIAL PIURA


ACL
CC. Archivo
Interesado

www.essalud.gob.pe

Av. Independencia s/n
Urb. Miraflores, Castilla
Piura, Perú
T: (073) 342420 / 34232

ANEXO 5

CORE CISCO CATALYST 4506-E



Features	Performance and Scalability
Centralized Wired Switching	Up to 928 Gbps
Capacity	
Wireless Termination Capacity	Up to 20 Gbps (software Roadmap)
Per-slot Switching Capacity	48 Gbps
Throughput	250 Mpps for IPv4, 125 Mpps for IPv6
IPv4 Routing Entries	256,000
IPv6 Routing Entries	128,000
Multicast Routes	32,000
CPU	Quad core; 2.0 GHz
CPU Queues	64

Synchronous Dynamic RAM (SDRAM)	4 GB
Nonvolatile RAM (NVRAM)	2 GB
Security and QoS Hardware Entries	128,000
Dynamic Host Configuration Protocol (DHCP) Snooping Entries	12,000
MAC Addresses	55,000
Active VLANs	4094
Address Resolution Protocol (ARP) Entries	47,000
Spanning Tree Protocol Instances	10,000
Switched Virtual Interfaces (SVIs)	4094
Switched Port Analyzer (SPAN)	Maximum of 8 bi-directional sessions

ANEXO 6

SWITCH ALCATEL LUCENT OMNISTACK LS 6224P



Características generales	
Tipo de dispositivo	Conmutador (switch)
Posibilidad de montaje en rack	sí
RAM	128 Mb
Memoria flash	16 Mb
Ranuras de interfaz adicional	2
Opciones avanzadas	
Peso	4.45 kg
Dimensiones (An X Al X Pr)	440 x 44 x 330 mm
Compatibilidad con estándares	Ethernet, IEEE 802.1p (Prioridad de etiquetas), IEEE 802.1Q (VLAN), IEEE 802.1d (Spanning Tree)

Soporte de IPv6	sí
Administración	
Interfaz web	sí
Soporte de Telnet	sí
Soporte SNMP	sí
Puerto de consola	sí
LAN	
Puertos	24 x Ethernet 10/100 Mbit/s
Ancho de banda	12.8 Gb/seg
Velocidad máxima de enlace	10/100/1000 Mbit/s
Voltaje	230 V
Fabricante	Nokia

ANEXO 7

TELEFONO IP YEALINK SIP-T23G



Descripción	
Número de líneas	3 líneas
BLF	No
Número de puertos RJ45	2 X 10/100/1000M Ethernet Ports
Gigabit	Sí
Conector para cascos	RJ9
Opciones avanzadas	
Número de cuentas SIP	Hasta 3 cuentas
PoE	Sí
Fuente de alimentación	No incluida

Teclados de expansión	No
Imagen	
Pantalla táctil	No
Pantalla color	No
Conexión	
Wifi	No
Bluetooth	No
Display	132x64-pixel graphical LCD
Manos Libres	Sí
VPN	Open VPN, IEEE802.1X

ANEXO 8 TELEFONO IP YEALINK SIP-T48G



Descripción	
Gigabit	Sí
Número de puertos RJ45	2 X 10/100/1000m Ethernet Ports
BLF	No
Número de líneas	16 líneas
Conector para cascos	RJ9 (SoportaEHS)
Opciones avanzadas	
Número de cuentas SIP	Hasta 16 cuentas
PoE	Sí
Fuente de alimentación	Opcional
Teclados de expansión	Soporta hasta 6 teclados de expansión
Imagen	
Pantalla táctil	Sí
Pantalla color	Sí
Conexión	
Wifi	No
Bluetooth	Sí (Mediante llave USB)
Display	7" 800 x 480-pixel color touch screen with backlight
Manos Libres	Sí
VPN	Open VPN, IEEE802.1X
USB	Sí
Características Adicionales	Skype for Business Online

ANEXO 9
CUESTIONARIO N° 1:

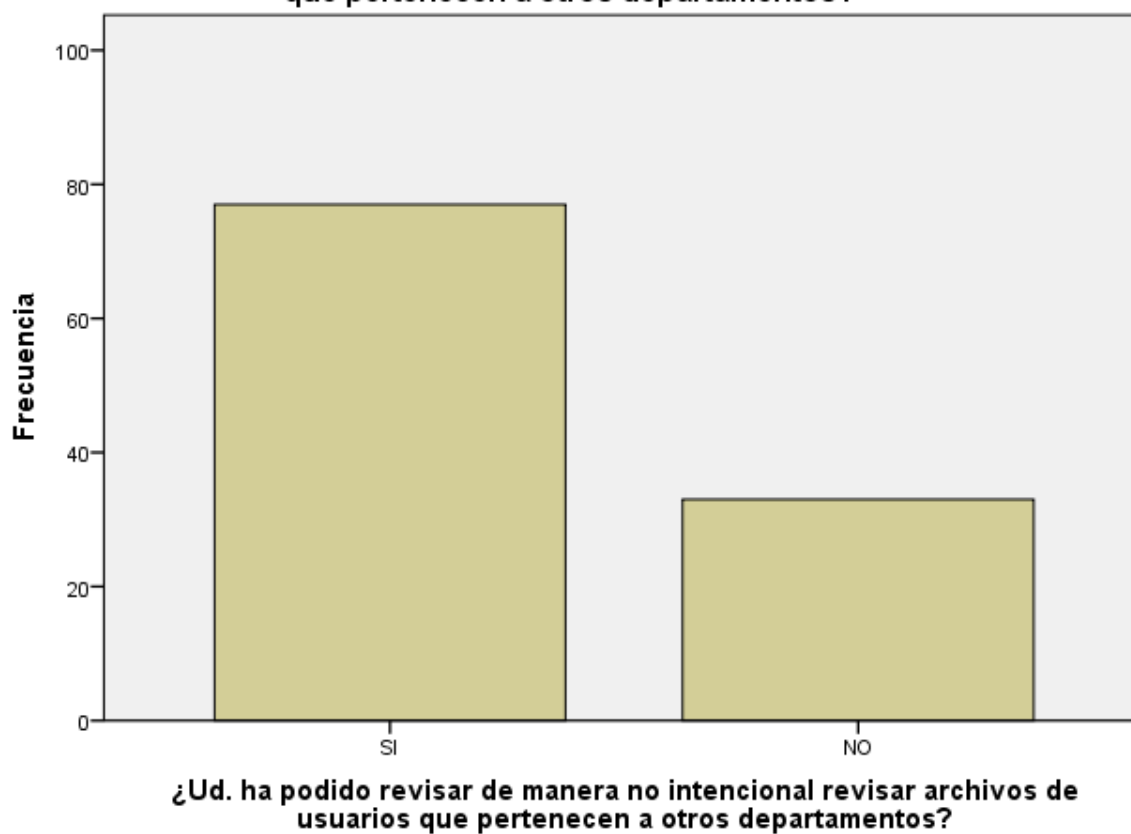
FECHA:

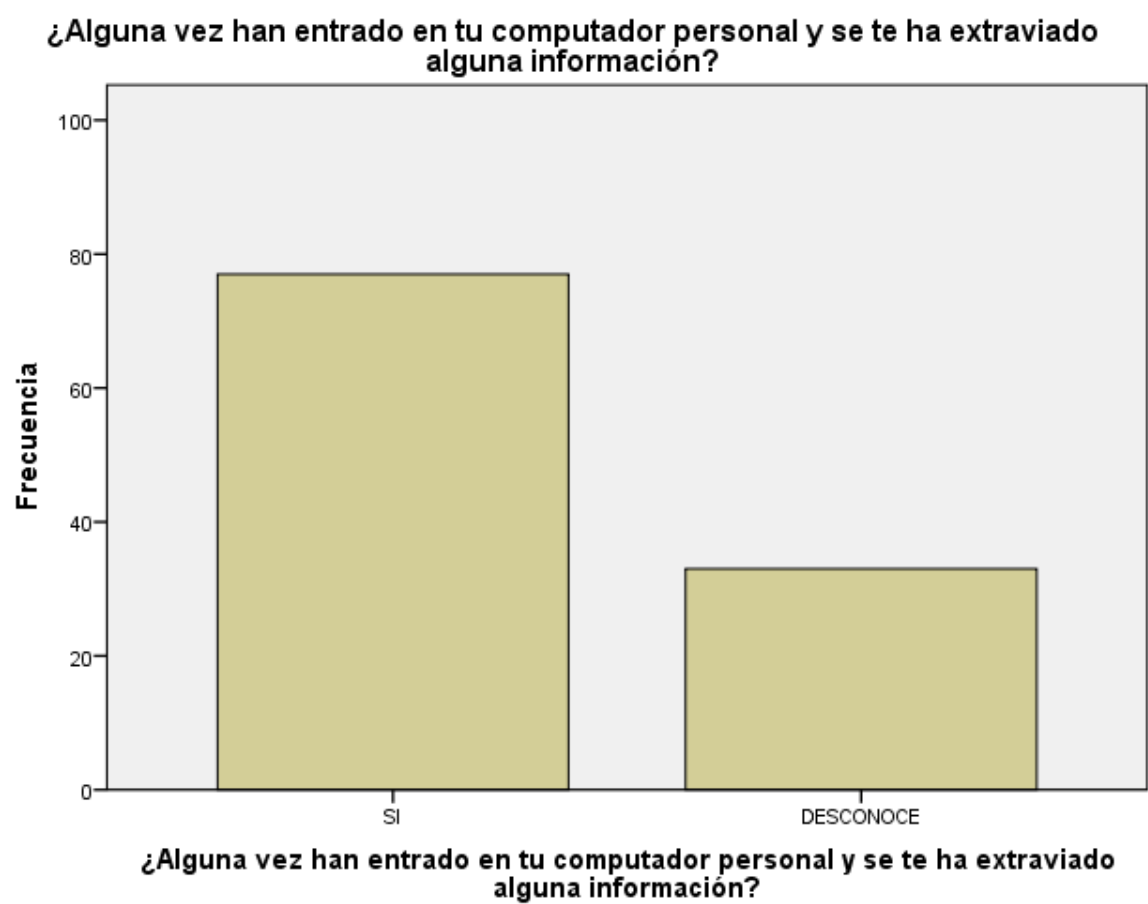
- 1. ¿Ud. ha podido revisar de manera no intencional revisar archivos de usuarios que pertenecen a otros departamentos?**
 - a. Si**
 - b. No**
- 2. ¿Alguna vez han entrado en tu computador personal y se te ha extraviado alguna información?**
 - a. Si**
 - b. No**
 - c. Desconoce**
- 3. ¿Ud. ha tenido problemas con la red ya sea de conexión, envió de datos o de congestión en la red?**
 - a. Si**
 - b. No**
- 4. ¿Alguna vez se ha propagado tu información de trabajo a usuarios de otro departamento?**
 - a. Si**
 - b. No**
 - c. Desconoce**
- 5. ¿Alguna vez se te ha perdido algún archivo cuando lo has compartido a través de la red?**
 - a. Si**
 - b. No**
 - c. Desconoce**

- 6. ¿Usuarios nuevos no han tenido donde conectarse a la red?**
- a. Si**
 - b. No**
 - c. Desconoce**
- 7. ¿Cree ud. que el ancho de banda que dispones es el ideal para tus operaciones diarias?**
- a. Si**
 - b. No**
 - c. Desconoce**
- 8. ¿Existen reclamos de los trabajadores del hospital por la demora en el acceso a los recursos de la red?**
- a. Si**
 - b. No**
 - c. Desconoce**

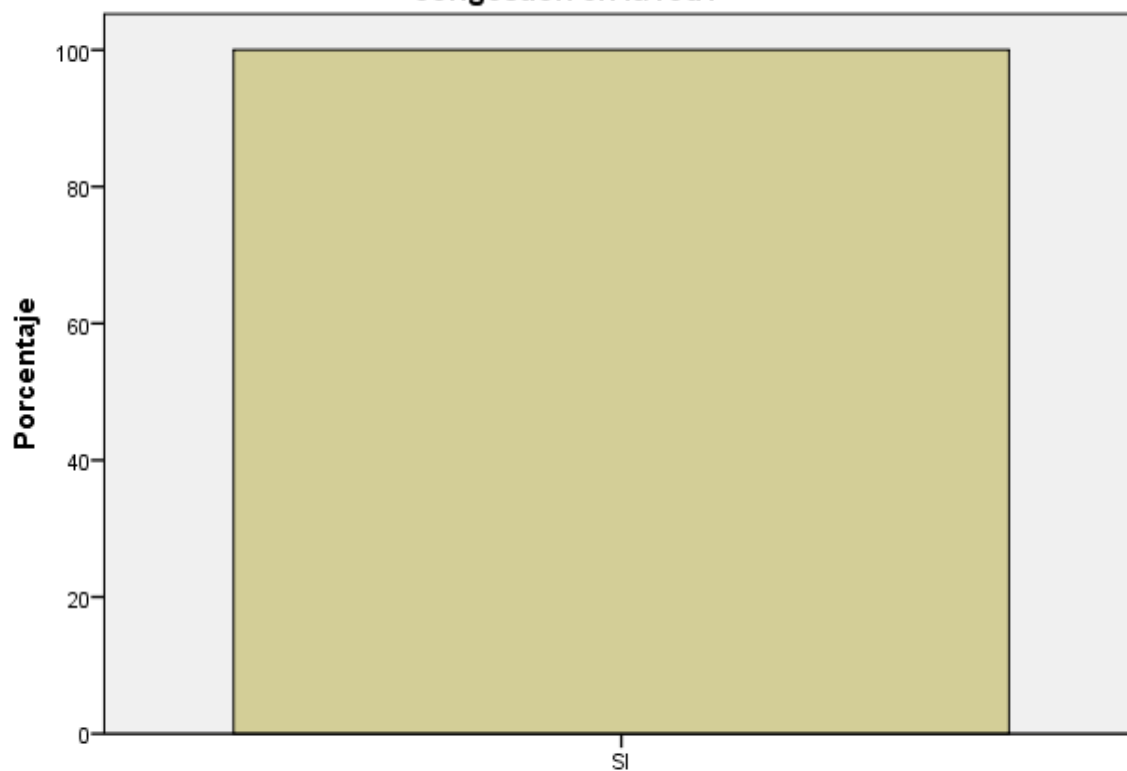
ANEXO 10
RESULTADOS DEL CUESTIONARIO N° 1:

¿Ud. ha podido revisar de manera no intencional revisar archivos de usuarios que pertenecen a otros departamentos?

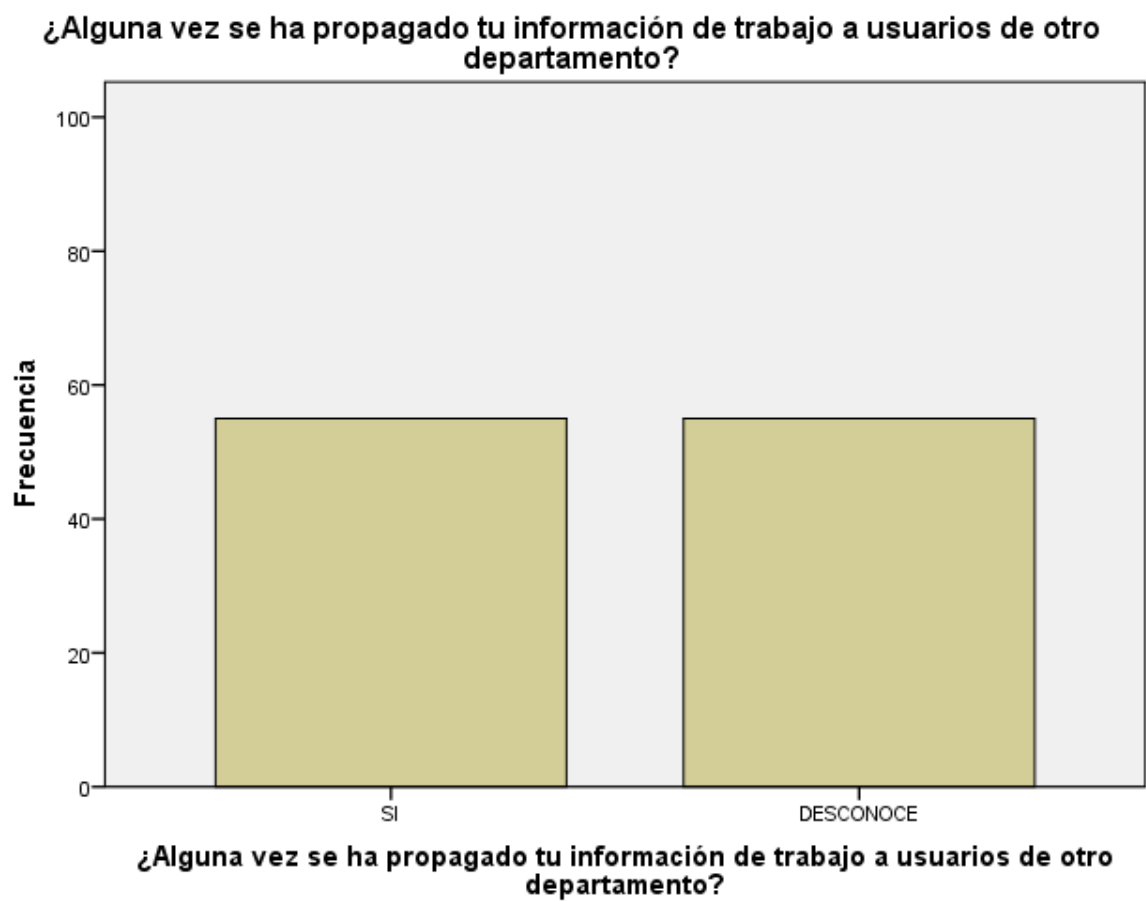




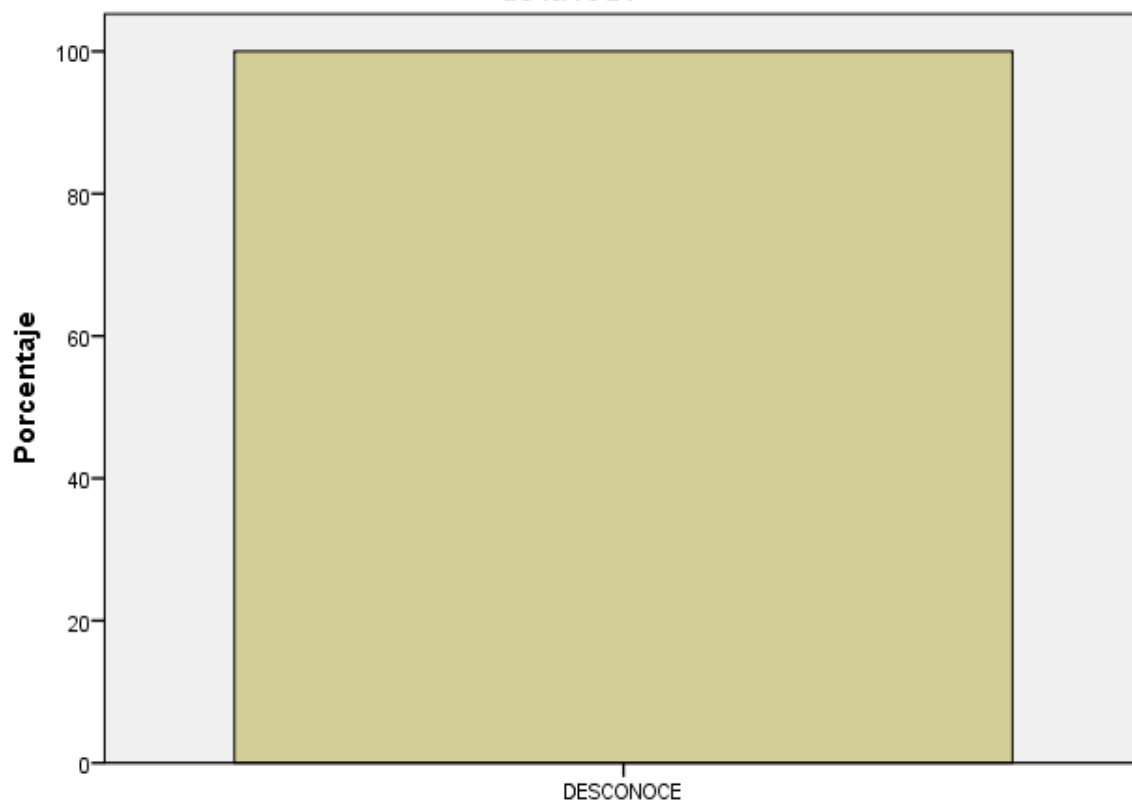
¿Ud. ha tenido problemas con la red ya sea de conexión, envío de datos o de congestión en la red?



¿Ud. ha tenido problemas con la red ya sea de conexión, envío de datos o de congestión en la red?



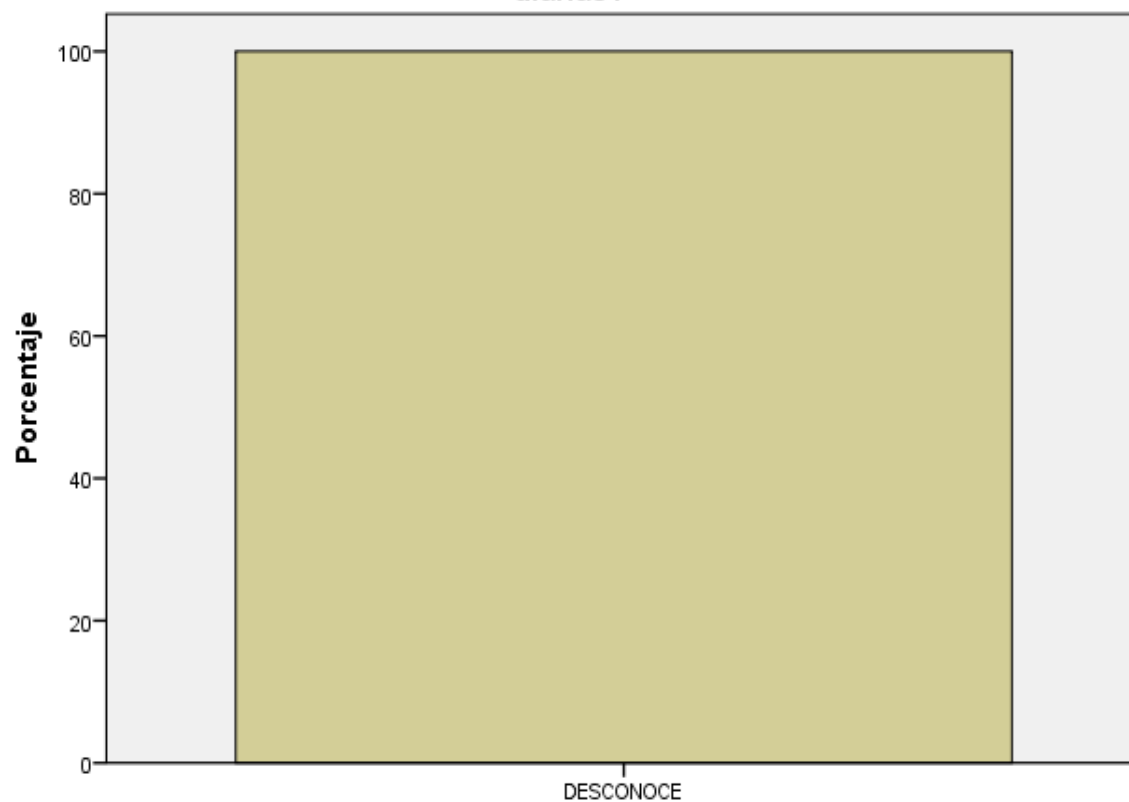
¿Alguna vez se te ha perdido algún archivo cuando lo has compartido a través de la red?



¿Alguna vez se te ha perdido algún archivo cuando lo has compartido a través de la red?

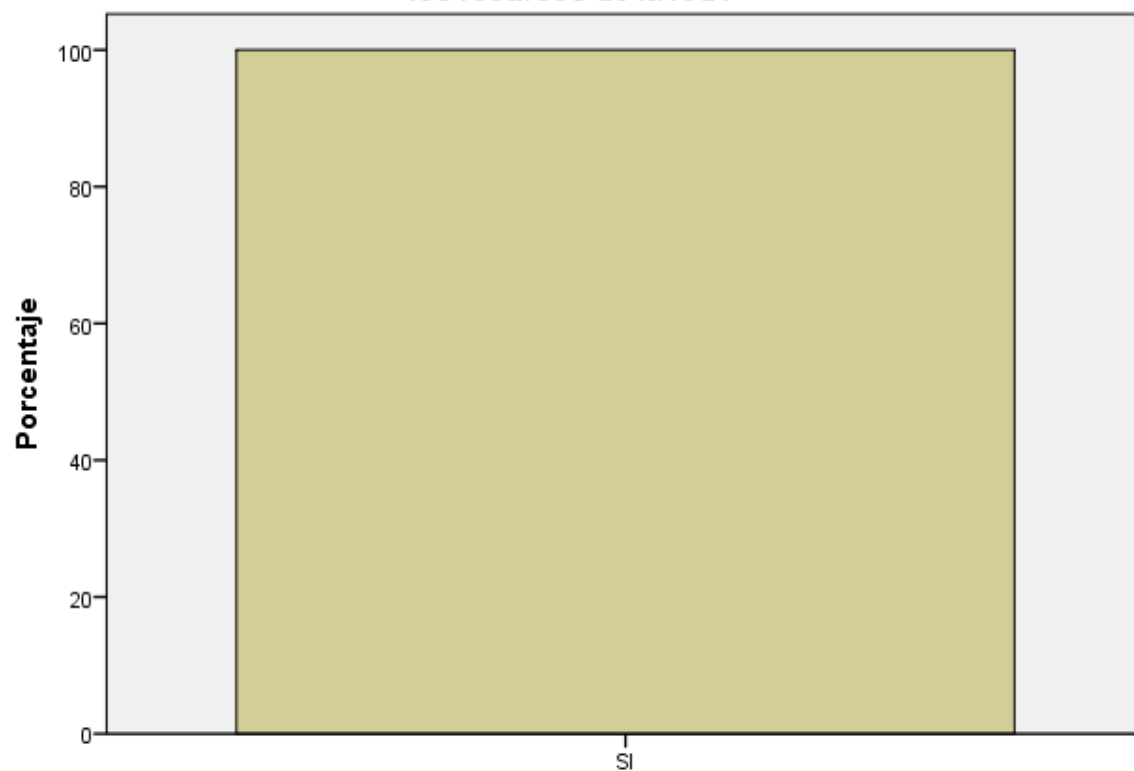


¿Cree ud. que el ancho de banda que dispones es el ideal para tus operaciones diarias?



¿Cree ud. que el ancho de banda que dispones es el ideal para tus operaciones diarias?

¿Existen reclamos de los trabajadores del hospital por la demora en el acceso a los recursos de la red?



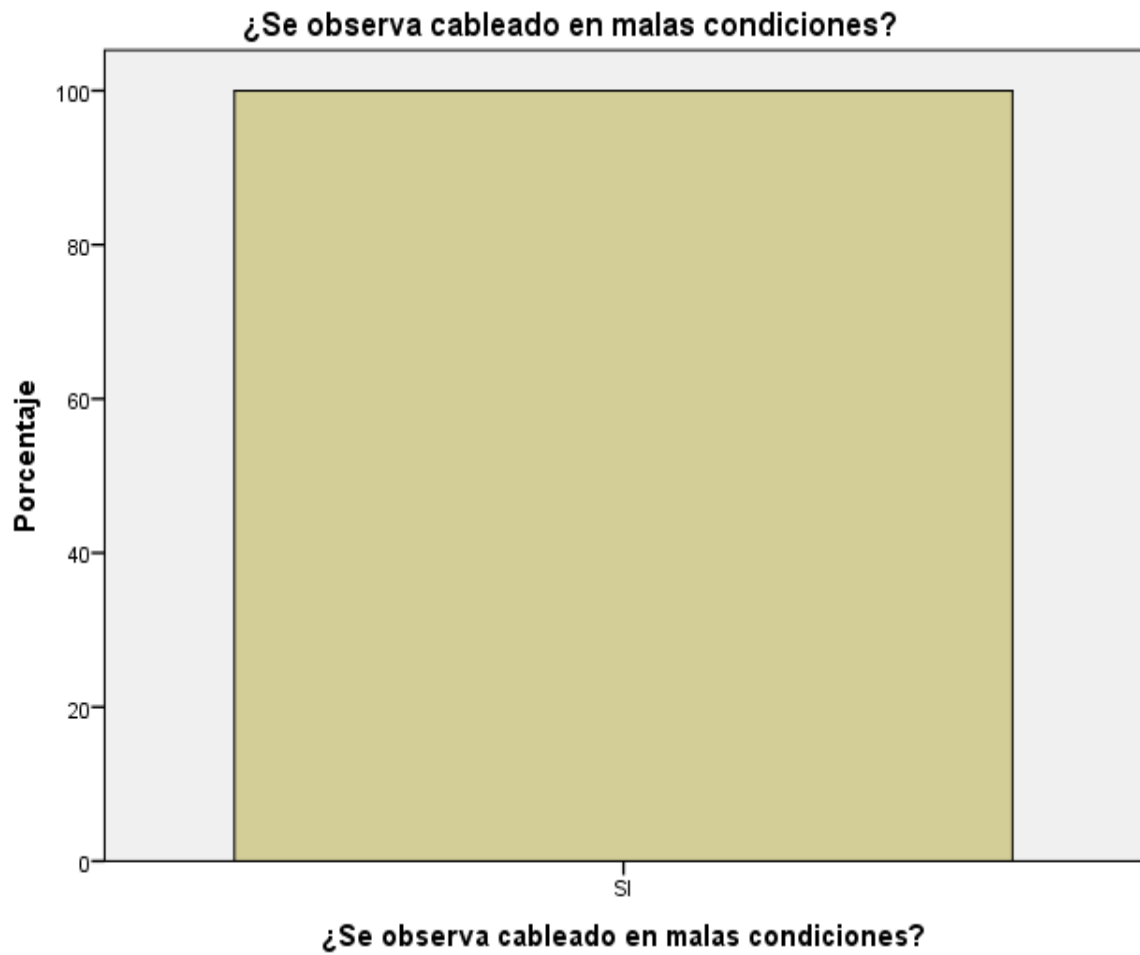
¿Existen reclamos de los trabajadores del hospital por la demora en el acceso a los recursos de la red?

ANEXO 11
GUÍA DE OBSERVACIÓN N° 1:

FECHA:

- 1. ¿Se observa cableado en malas condiciones?**
 - a. SI**
 - b. NO**
- 2. ¿Los equipos de comunicación se encuentran expuesto?**
 - a. SI**
 - b. NO**
- 3. ¿Los equipos de comunicación podrían ser fácilmente manipulados por usuarios no autorizados?**
 - a. SI**
 - b. NO**
- 4. ¿Existen puntos de red que no se encuentran en funcionamiento?**
 - a. SI**
 - b. NO**
- 5. Como calificaría el estado del cableado de red:**
 - a. Bueno**
 - b. Regular**
 - c. Malo**
- 6. ¿Los usuarios se quejan de los problemas con la red?**
 - a. SI**
 - b. NO**

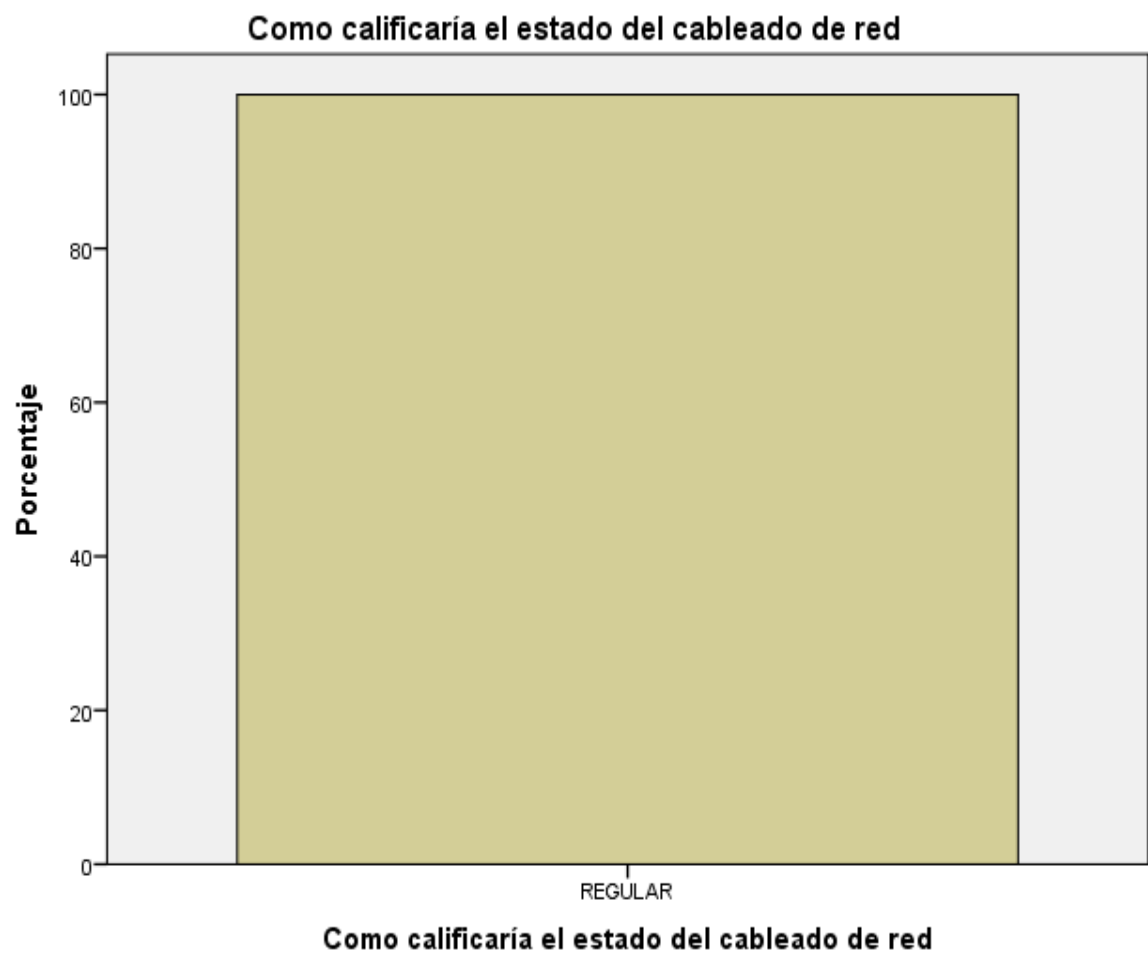
ANEXO 12
RESULTADOS DE LA GUÍA DE OBSERVACIÓN N° 1:

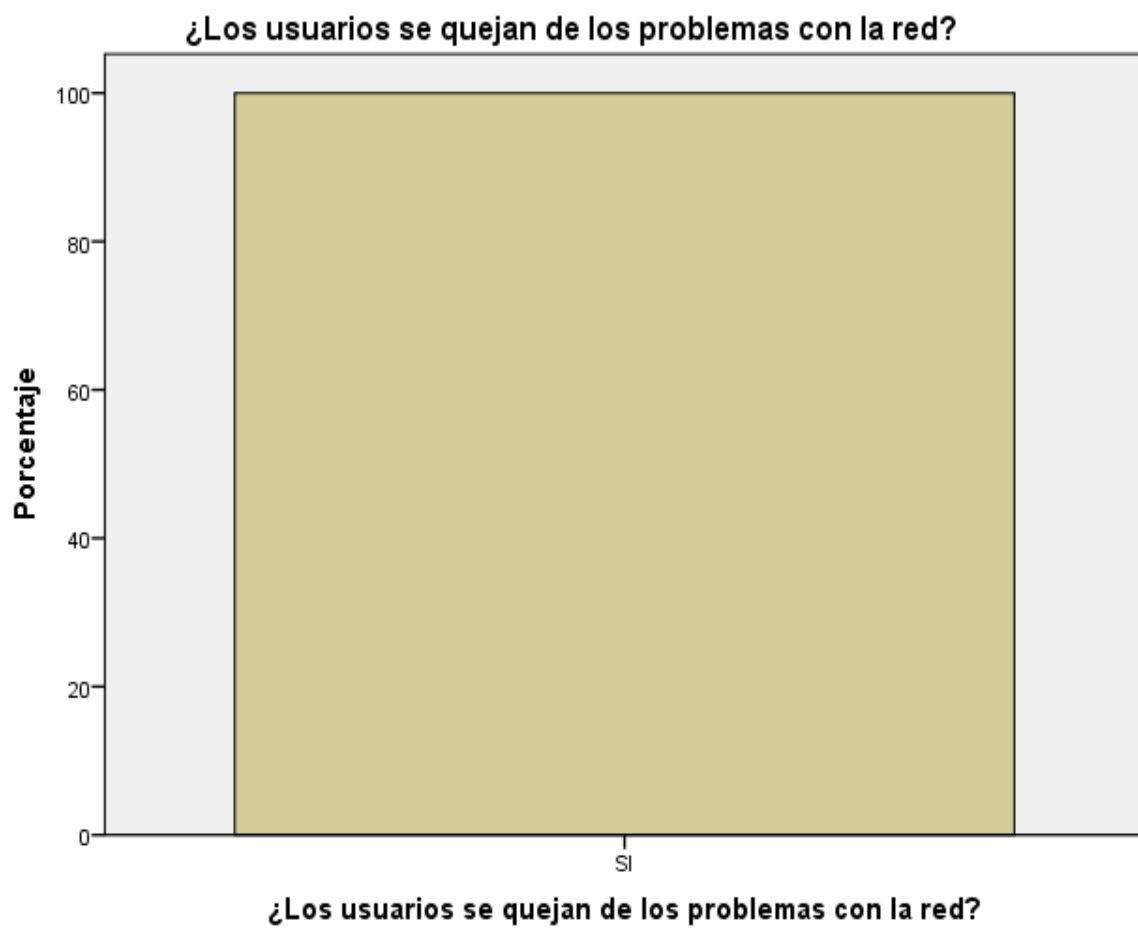












ANEXO 13

CREACION DE VLANs

Enable

configure terminal

do vlan database

vlan 10 name V_SOP //SOPORTE INFORMATICO

vlan 20 name V_DOS //DOSIS UNITARIA

vlan 30 name V_IPO //IPO

vlan 40 name V_HIS //HISTORIAS CLINICAS

vlan 50 name V_CONT //CONTROL TIEMPO

vlan 60 name V_CUE //CUERPO MEDICO

vlan 70 name V_CEP //CEPRIT

vlan 80 name V_PRE //PRESTACIONES ECONÓMICAS

vlan 90 name V_ASE //ASESORÍA JURÍDICA

vlan 100 name V_BAN //BANCO DE SANGRE

vlan 110 name V_ESS //ESSALUD EN LINEA

vlan 120 name V_CONS //CONSULTORIOS

vlan 130 name V_CAJ //CAJA FACTURACIÓN

vlan 140 name V_VOIP //VOZ SOBRE IP

exit

ANEXO 14

CONFIGURACIÓN DE EQUIPOS

SWITCHES

SW_SOPORTE_INFORMATICO

Enable

configure terminal

int range fa0/1-10

switchport access vlan 10

ex

int range fa0/11-20

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_DOSIS_UNITARIA

Enable

configure terminal

int range fa0/1-9

switchport access vlan 20

ex

int range fa0/10-18

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_IPO

Enable

configure terminal

int range fa0/1-6

switchport access vlan 30

ex

int range fa0/7-12

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_HISTORIA_CLINICAS

Enable

configure terminal

int range fa0/1-9

switchport access vlan 40

ex

int range fa0/10-18

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_CONTROL_TIEMPO

Enable

configure terminal

int range fa0/1-6

switchport access vlan 50

ex

int range fa0/7-12

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_CUERPO_MÉDICO

Enable

configure terminal

int range fa0/1-10

switchport access vlan 60

ex

int range fa0/11-20

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_CEPRIT

Enable

configure terminal

int range fa0/1-10

switchport access vlan 70

ex

int range fa0/11-20

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_PRESTACIONES_ECONÓMICAS

Enable

configure terminal

int range fa0/1-9

switchport access vlan 80

ex

int range fa0/10-18

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_ASESORÍA_JURÍDICA

Enable

configure terminal

int range fa0/1-6

switchport access vlan 90

ex

int range fa0/7-12

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_BANCO_DE_SANGRE

Enable

configure terminal

int range fa0/1-9

switchport access vlan 100

ex

int range fa0/10-18

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_ESSALUD_EN_LINEA

Enable

configure terminal

int range fa0/1-5

switchport access vlan 110

ex

int range fa0/6-10

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_CONSULTORIOS

Enable

configure terminal

int range fa0/1-10

switchport access vlan 120

ex

int range fa0/11-20

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_CONSULTORIOS

Enable

configure terminal

int range fa0/1-10

switchport access vlan 120

ex

int range fa0/11-20

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

SW_CAJA_FACTURACIÓN

Enable

configure terminal

int range fa0/1-10

switchport access vlan 130

ex

int range fa0/11-20

switchport voice vlan 140

ex

int range fa0/23-24

sw mode trunk

sw native vlan 1

no sh

ex

ex

copy run start

ROUTER

Enable

Configure terminal

int fa0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.240

int fa0/0.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.240

int fa0/0.30

encapsulation dot1Q 30

ip address 192.168.30.1 255.255.255.240

int fa0/0.40

encapsulation dot1Q 40

ip address 192.168.40.1 255.255.255.240

int fa0/0.50

encapsulation dot1Q 50

ip address 192.168.50.1 255.255.255.240

int fa0/0.60

encapsulation dot1Q 60

ip address 192.168.60.1 255.255.255.240

int fa0/0.70

encapsulation dot1Q 70

ip address 192.168.70.1 255.255.255.240

int fa0/0.80

```
encapsulation dot1Q 80
ip address 192.168.80.1 255.255.255.240
int fa0/0.90
encapsulation dot1Q 90
ip address 192.168.90.1 255.255.255.240
int fa0/0.100
encapsulation dot1Q 100
ip address 192.168.100.1 255.255.255.240
int fa0/0.110
encapsulation dot1Q 110
ip address 192.168.110.1 255.255.255.240
int fa0/0.120
encapsulation dot1Q 120
ip address 192.168.120.1 255.255.255.240
int fa0/0.130
encapsulation dot1Q 130
ip address 192.168.130.1 255.255.255.240
int fa0/0.140
encapsulation dot1Q 140
ip address 192.168.140.1 255.255.255.128
ex
int fa0/0
ip add 192.168.140.1 255.255.255.0
no shut
ex
```



```

ip dhcp pool voz
net 192.168.140.0 255.255.255.0
default-router 192.168.140.1
option 150 ip 192.168.140.1
ex
ex
wr
telephony-service
max-dn 144
max-ephones 42
ip source-address 192.168.140.1 port 2000
auto assign 1 to 144
ex
ex
wr
-----telefonos vlan 10-----
conf t
ephone-dn 1
number 11
ephone-dn 2
number 12
ephone-dn 3
number 13
ephone-dn 4
number 14

```

ephone-dn 5

number 15

ephone-dn 6

number 16

ephone-dn 7

number 17

ephone-dn 8

number 18

ephone-dn 9

number 19

ephone-dn 10

number 20

-----telefonos vlan 20-----

ephone-dn 11

number 21

ephone-dn 12

number 22

ephone-dn 13

number 23

ephone-dn 14

number 24

ephone-dn 15

number 25

ephone-dn 16

number 26

ephone-dn 17

number 27

ephone-dn 18

number 28

ephone-dn 19

number 29

ephone-dn 20

number 30

-----telefonos vlan 30-----

ephone-dn 21

number 31

ephone-dn 22

number 32

ephone-dn 23

number 33

ephone-dn 24

number 34

ephone-dn 25

number 35

ephone-dn 26

number 36

ephone-dn 27

number 37

ephone-dn 28

number 38

ephone-dn 29

number 39

ephone-dn 30

number 40

-----telefonos vlan 40-----

ephone-dn 31

number 41

ephone-dn 32

number 42

ephone-dn 33

number 43

ephone-dn 34

number 44

ephone-dn 35

number 45

ephone-dn 36

number 46

ephone-dn 37

number 47

ephone-dn 38

number 48

ephone-dn 39

number 49

ephone-dn 40

number 50

-----telefonos vlan 50-----

ephone-dn 41

number 51

ephone-dn 42

number 52

ephone-dn 43

number 53

ephone-dn 44

number 54

ephone-dn 45

number 55

ephone-dn 46

number 56

ephone-dn 47

number 57

ephone-dn 48

number 58

ephone-dn 49

number 59

ephone-dn 50

number 60

-----telefonos vlan 60-----

ephone-dn 51

number 61

ephone-dn 52

number 62

ephone-dn 53

number 63

ephone-dn 54

number 64

ephone-dn 55

number 65

ephone-dn 56

number 66

ephone-dn 57

number 67

ephone-dn 58

number 68

ephone-dn 59

number 69

ephone-dn 60

number 70

-----telefonos vlan 70-----

ephone-dn 61

number 71

ephone-dn 62

number 72

ephone-dn 63

number 73

ephone-dn 64

number 74

ephone-dn 65

number 75

ephone-dn 66

number 76

ephone-dn 67

number 77

ephone-dn 68

number 78

ephone-dn 69

number 79

ephone-dn 70

number 80

-----telefonos vlan 80-----

ephone-dn 71

number 81

ephone-dn 72

number 82

ephone-dn 73

number 83

ephone-dn 74

number 84

ephone-dn 75

number 85

ephone-dn 76

number 86

ephone-dn 77

number 87

ephone-dn 78

number 88

ephone-dn 79

number 89

ephone-dn 80

number 90

-----telefonos vlan 90-----

ephone-dn 81

number 91

ephone-dn 82

number 92

ephone-dn 83

number 93

ephone-dn 84

number 94

ephone-dn 85

number 95

ephone-dn 86

number 96

ephone-dn 87

number 97

ephone-dn 88

number 98

ephone-dn 89

number 99

ephone-dn 90

number 100

-----telefonos vlan 100-----

ephone-dn 91

number 101

ephone-dn 92

number 102

ephone-dn 93

number 103

ephone-dn 94

number 104

ephone-dn 95

number 105

ephone-dn 96

number 106

ephone-dn 97

number 107

ephone-dn 98

number 108

ephone-dn 99

number 109

ephone-dn 100

number 110

-----telefonos vlan 110-----

ephone-dn 101

number 111

ephone-dn 102

number 112

ephone-dn 103

number 113

ephone-dn 104

number 114

ephone-dn 105

number 115

ephone-dn 106

number 116

ephone-dn 107

number 117

ephone-dn 108

number 118

ephone-dn 109

number 119

ephone-dn 110

number 120

-----telefonos vlan 120-----

ephone-dn 111

number 121

ephone-dn 112

number 122

ephone-dn 113

number 123

ephone-dn 114

number 124

ephone-dn 115

number 125

ephone-dn 116

number 126

ephone-dn 117

number 127

ephone-dn 118

number 128

ephone-dn 119

number 129

ephone-dn 120

number 130

-----telefonos vlan 130-----

ephone-dn 121

number 131

ephone-dn 122

number 132

ephone-dn 123

number 133

ephone-dn 124

number 134

ephone-dn 125

number 135

ephone-dn 126

number 136

ephone-dn 127

number 137

ephone-dn 128

number 138

ephone-dn 129

number 139

ephone-dn 130

number 140